サーバプロテクションサービス
【管理者用】運用マニュアル

フルモデル（仮想パッチ＋ウイルス対策）編

株式会社 大塚商会

Vol.SPS95 2017/12/01 1.2版

はじめに

ここでは、本マニュアルについて説明します。

対象読者

社内サーバ管理者、セキュリティ管理者

マニュアルの目的

本マニュアルは、サーバプロテクションサービスの機能および運用方法を理解していただくことを目的にしています。

マニュアル内の記述について

お客様がご使用になるOS環境により、表示・表現が本マニュアルと異なる場合がありますのでご了承ください。

＊Windows Server® 2003、Windows Server® 2008、Windows Server® 2012は、米国Microsoft Corporation の米国およびその他の国における登録商標または商標です。

＊Deep Securityは、トレンドマイクロ株式会社の登録商標です。

＊記載されている会社名および商品名は、各社の商標または登録商標です。なお、本文中では、™!やRなどの記号は使用しておりません。

＊記載されている商品名は特に断りがない限り日本語版です。

マニュアル内で使用している記号

略称	目的
『 』	マニュアルの名称を示します。
「 」	ウィンドウの名称およびメッセージ、製品名、参照先を示します。
[ ]	メニューやタブの名称と、ボタンおよびキーを示します。
🗗	ウィンドウ、ダイアログ、コンソール画面などを示します。
	操作および運用上のヒントを示します。
	操作および運用上の注意を示します。
	操作および運用上の関連事項を示します。
	マニュアル内、または別冊マニュアルの参照先を示します。

目次

1.サービスについて

この章では、基本用語、機能、動作環境、導入から運用までの流れについて説明します。

1-1.基本用語

本サービスで使われる基本用語は、次の表のとおりです。

用語	説明
マネージャー	対象サーバの管理と各種設定を保存するサーバです。
エージェントプログラム	対象サーバにインストールするプログラムです。
エージェント	本サービス管理下のサーバOSです。
管理コンソール	マネージャーに接続して、各種ログやレポートの表示を行うコンソールです。 Internet Explorerを使用します。
管理者ID	本サービス契約時に郵送した、管理コンソールへのログオンアカウントです。
侵入防御	パッチが適用されるまでの間、既知の脆弱性に対する様々な攻撃コードにさらされないようにします。 ※Deep Security 9.0 以降より、”Deep Packet Inspection”および”DPI” が”侵入防御”に名称変更されました。
仮想パッチ	ベンダーから正式なパッチが提供されるまでの一時的な対策として、仮想的に脆弱性を修正するプログラムです。
IPS	侵入防御システム。コンピュータへの不正な侵入の兆候を検知し、防御します。
Webレピュテーション	ウイルスに感染する危険性のあるWebサイトへの接続を自動的にブロックする機能です。

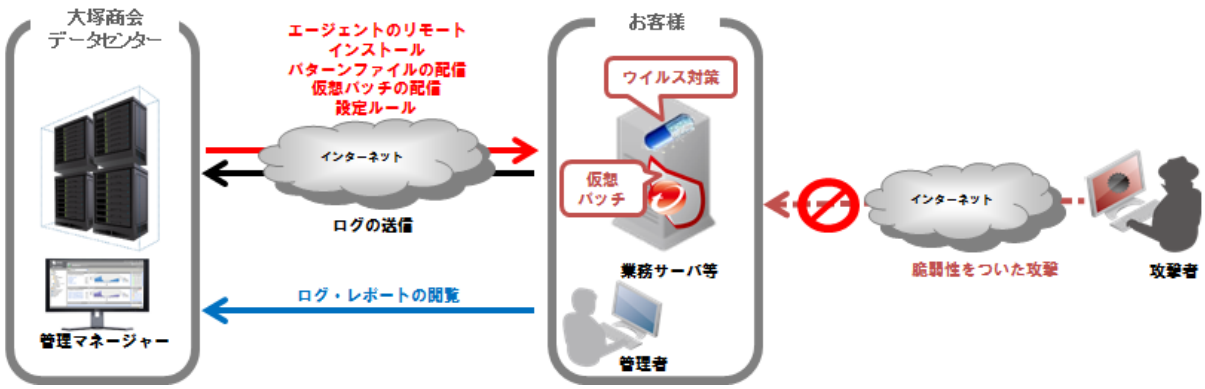
1-2.サービス内容

・仮想パッチ:トレンドマイクロ法人向け総合セキュリティソフト「Deep Security」の仮想パッチ(侵入防御)機能を ASP サービスとして提供します。

・ウイルス対策:トレンドマイクロ法人向け総合セキュリティソフト「Deep Security」の不正プログラムの駆除機能を ASP サービスとして提供します。

・お客様による管理サーバの設置・運用やライセンスの管理は不要で、エージェントとなるサーバ OS へのエージェントプログラムのインストールだけでご利用できます。

・管理コンソール:ログの参照やレポートの生成とダウンロードが可能です。



1-2-1.本サービスでご提供する内容

本サービスでは以下のような環境をご提供します。

① インターネットブラウザーで閲覧するセキュリティ適用状況の確認画面(管理コンソール)

② 仮想パッチエージェントプログラム(Deep Security Agent)

③ ウイルス対策エージェントプログラム(Deep Security Agent)

④ 関連する各種マニュアル類一式

※ ④関連する各種マニュアル類一式は、ご契約時にご案内するポータルサイトよりダウンロードできます。

1-2-2.主なサービス概要

・仮想パッチ機能
OSの脆弱性を狙った攻撃に対し、その脆弱性を狙った攻撃コードを見分け、攻撃をブロックするために必要な仮想パッチを適用します。また、この機能は弊社の推奨設定値にて定期的に脆弱性と適応済みセキュリティパッチをスキャンし、自動的に仮想パッチの適用・除去を行います。

・ウイルス対策機能
不正プログラムに対するリアルタイム検索及び予約検索を行います。不正プログラムを検出した場合は自動的に処理を行います。処理に失敗した場合は、別途手動での処理が必要です。また、エージェント側での手動検索は実行できません。

・Webレピュテーション
不正プログラムに感染する可能性が高いWebサイトへの接続制御を行います。不正プログラムに感染する可能性が高いWebサイトに接続しようとした場合は、ブロック画面が表示されます。

・ウィジェット
ウィジェットは管理コンソールのトップページに表示される情報パネルのことです。情報の種類を選択したり、レイアウトを変更したりすることが可能です。

参照 3.3.2ウィジェットの追加/削除

・サーバ情報の参照
エージェントとなっているサーバのOSや、管理のステータス、アップデートの状況などの情報を収集し、エージェントごとに閲覧できます。

参照 3.5サーバ情報の参照

・各種レポートの表示機能
本サービスでは、エージェントとなっているサーバOSでのDeepSecurity Agentの情報を収集し、各種レポートを表示します。
収集した情報をもとに、過去4週間分の仮想パッチによる攻撃防御や不正プログラムの検出状況などをレポートで確認できます。
・アラートレポート ・不正プログラム対策レポート ・攻撃レポート ・侵入防御レポート ・概要レポート 他

参照 3.6レポート

1-3.動作環境やご利用条件の概要

1-3-1.システム要件

対応 OS	Microsoft Windows Server 2012 R2（64 ビット）
	Microsoft Windows Server 2012（64 ビット）
	Microsoft Windows Server 2008 R2（64 ビット）
	Microsoft Windows Server 2008（32 ビット/64 ビット）
	Microsoft Windows Server 2003 R2 SP2（32 ビット/64 ビット）
	Microsoft Windows Server 2003 SP2（32 ビット/64 ビット）
仮想環境	Agent をインストールするゲスト OS がサポート対象であれば、ハイパーバイザー/ホストの種類に関わらずサポート対象。ただし、仮想環境のみで発生し物理環境で再現できない問題は、対応されない可能性があります。
メモリ	1GB(最小)、2GB(推奨)
HDD	500MB 以上のハードディスク空き容量 （不正プログラム対策機能を使用する場合は1GB 以上を推奨）
ネットワークプロトコルおよびサービス	TCP/IP、Microsoft Network、RPC サービスがインストール先サーバで実行されていること

※記載のシステム要件は 2016 年 5 月現在のものです

1-3-2.ご利用条件

以下、ご利用にあたっての注意事項の概略です。（詳しくは『ご利用条件』をご参照下さい。）

1.本サービスの開始に当たり、サーバへのインストールは弊社よりリモートで行います（初期費用が発生いたします）。弊社からのリモート接続ができない場合には、弊社エンジニアが作業を実施します。その際は別途有償となります。

2.リモート接続によるエージェントインストール作業は9:00～17:30の間に限られます。

3.エージェントソフトについて

（1） ご提供する機能は仮想パッチとウイルス対策のみとなります。

（2） ルールの割り当ては、推奨スキャン機能での提供となります。

・推奨スキャンは毎週木曜日、金曜日、土曜日、日曜日の0:00～8:00に実行します。（5:00～6:00の間はサーバ再起動のため、除く）

・該当の時間にサーバが停止していた場合は、次の推奨スキャンのタイミングに実行されます。

（3） 緊急度の高い脆弱性ルールがリリースされた場合、事前の予告なく推奨スキャンを実行する場合があります。

（4） 管理マネージャーからのレポート閲覧、レポート作成は、弊社が定めるサーバメンテナンス時間内は出来ません。

（5） 管理マネージャーからのレポート閲覧、レポート作成は過去4週間分になります。

（6） 他のウイルス対策ソフトとの同居は不可となります。本サービスのウイルス対策に乗り換える場合は、お客様自身でアンインストールして下さい。

（7） サーバにエージェントをインストールする場合、ネットワークの一時的な切断、またはOSのネットワークドライバが他のプログラムによって使われている場合は、OSの再起動を求められる場合があります。

（8） 以下の環境でDeep Security エージェントの動作はサポート対象外となります。

・Network Load Balanceを構成しているサーバ

・Windows Server 2012 Server Core

・Windows Server 2008 Server Core

（9） エージェントソフトから直接インターネットへの443/TCP、4120/TCP、4122/TCPへアクセスが可能になっている必要があります。

1-3-3.ご利用時の注意事項

※ 本サービスの実施により、セキュリティパッチの適応を不要とするものではありません。お客様で計画的にセキュリティパッチの適用を実施していただく必要があります。

※ 本サービスは、外部から不正アクセスやウイルスからの防御を完全にお約束するものではありません。ウイルス等の損害については、一切保証致しません。導入後の状況は、お客様自身で管理画面からご確認ください。

2.お客様マイページについて

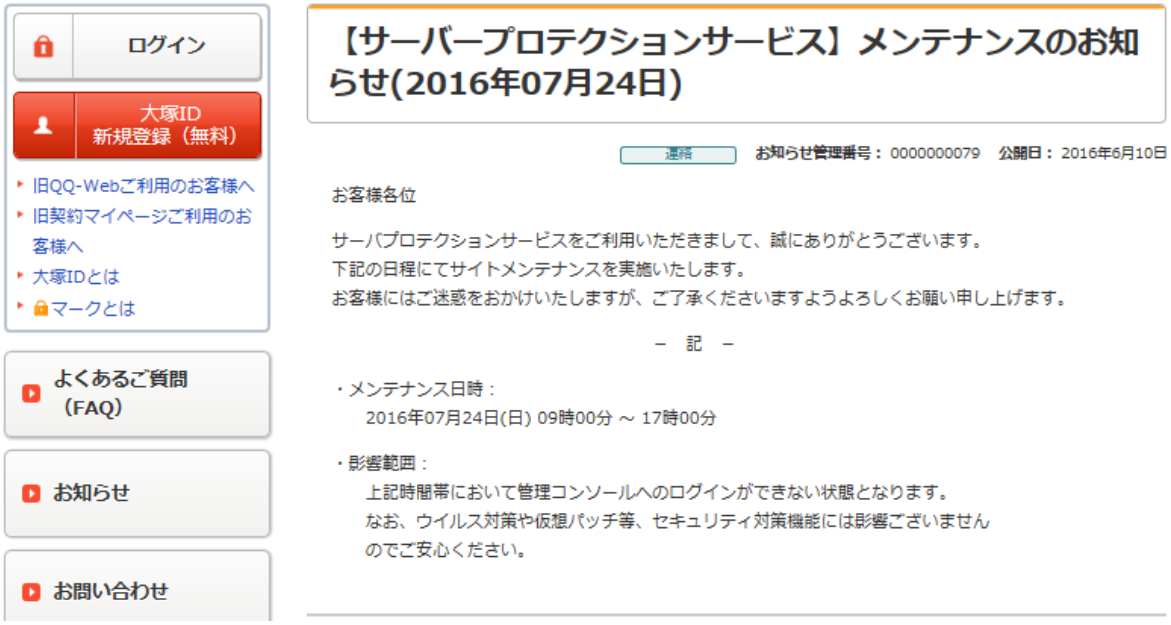
この章では、サーバプロテクションサービスのお客様マイページについて説明します。
お客様マイページでは、管理者様宛のお知らせのご確認や、マニュアルのダウンロードを行っていただくことができます。また、サーバプロテクションサービス管理コンソールへのログインもお客様マイページから行っていただきます。
お客様マイページのURL及びサーバプロテクションサービスのログイン用IDとパスワードは「サーバプロテクションサービス登録完了のお知らせ」にも記載されておりますので、併せてご確認ください。

2-1.お知らせ

サーバプロテクションサービスに関するお知らせが発生した場合、お客様マイページから管理者様へお知らせいたします。「お知らせ」とは、メンテナンス情報、障害情報、誤検知情報、バージョンアップ情報等を指します。

① お客様マイページのURL(https://mypage.otsuka-shokai.co.jp/sps)へアクセスします。

② 「お知らせ」の詳細が掲示されているページが開きます。



2-2.各種手順書のダウンロード

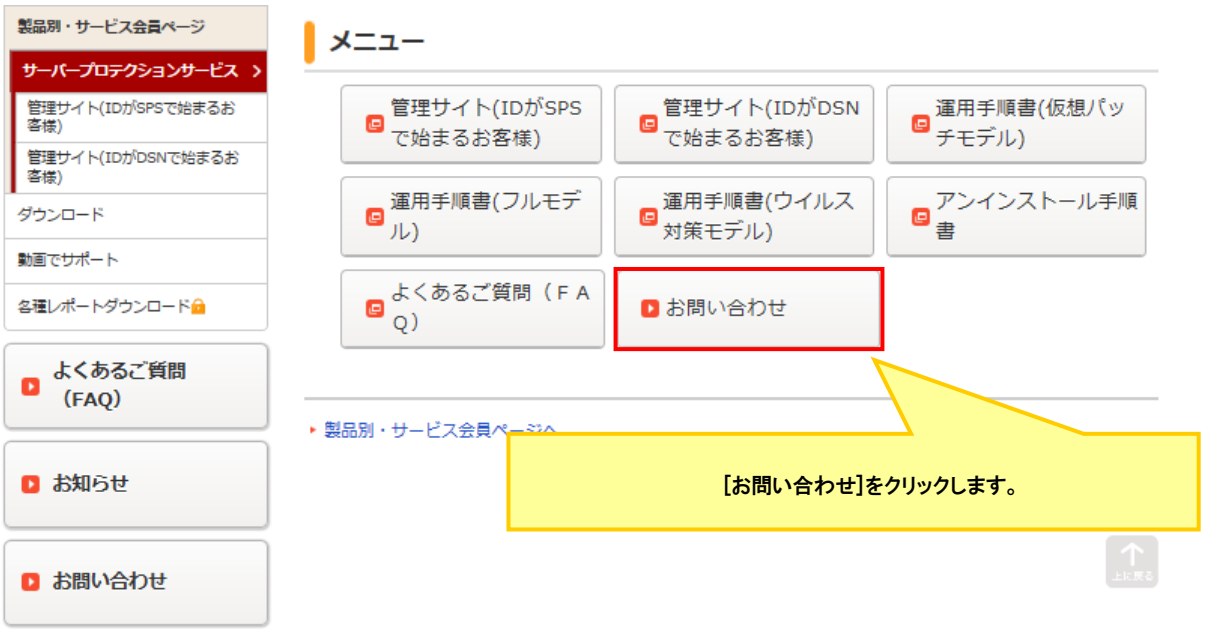
管理者様向けの各種手順書はお客様マイページからダウンロードいただけます。

① お客様マイページのURL(https://mypage.otsuka-shokai.co.jp/sps)へアクセスします。

2-3.お問い合わせ

サーバプロテクションサービスについてご不明点がある場合、お問い合わせいただく窓口の情報をお客様マイページからご確認いただけます。

① お客様マイページのURL(https://mypage.otsuka-shokai.co.jp/sps)へアクセスします。



② ログイン画面が表示されます。 ※既にログイン済の場合は表示されません。

③　お問合せフォームが表示されます。

3.管理コンソールについて

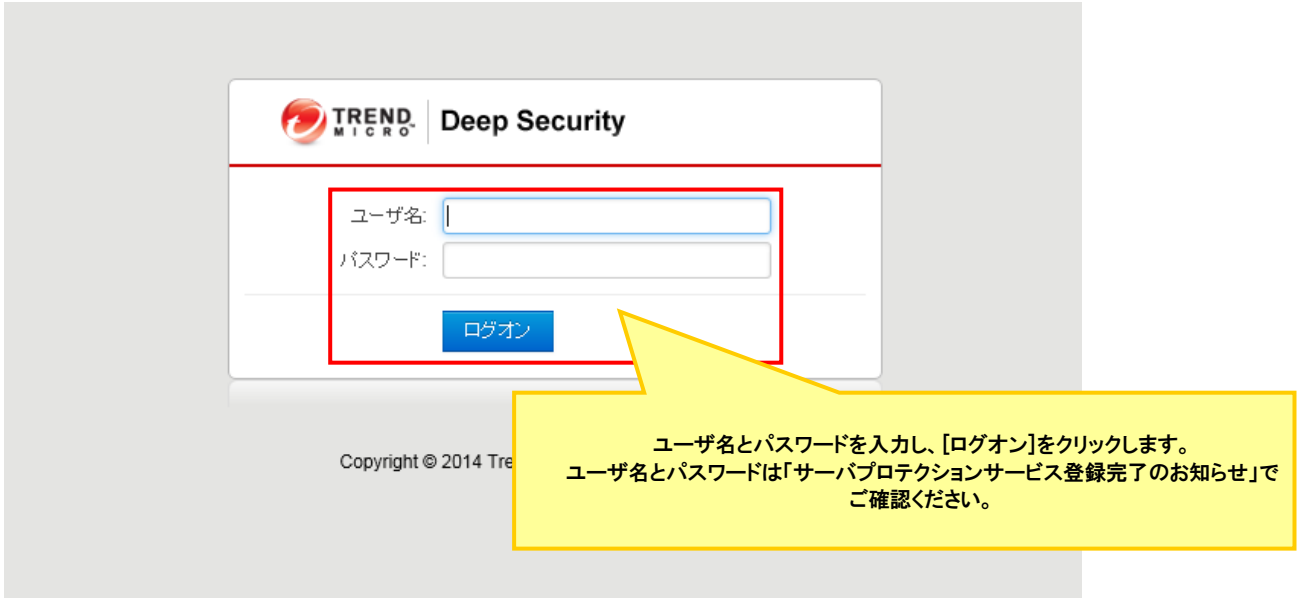
この章では、サーバプロテクションサービスの管理コンソールについてご説明いたします。

3-1.ログオン

お客様マイページから、サーバプロテクションサービスの管理コンソールにログオンします。

① お客様マイページのURL(https://mypage.otsuka-shokai.co.jp/sps)へアクセスします。

① サーバプロテクションサービス管理コンソールのログオン画面が開きます。



② ログインに成功すると はじめに 画面が開きます。

※次回以降表示不要の場合は、画面左下のチェックを外してください。

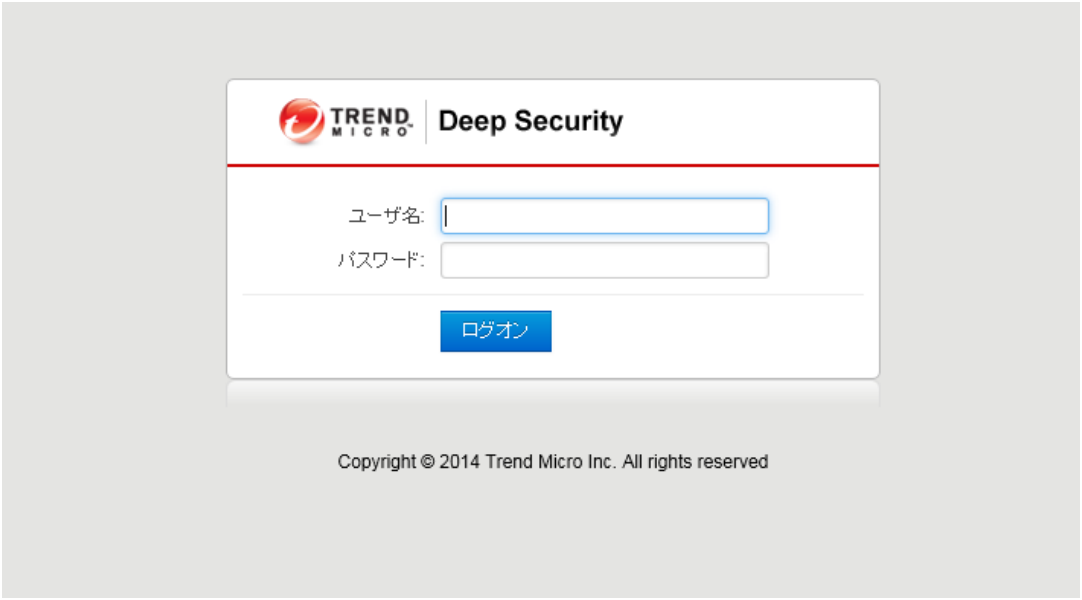
③ サーバプロテクションサービス管理コンソールが開き、ダッシュボード画面が表示されます。

3-2.ログオフ

サーバプロテクションサービス管理コンソールでの作業が終了したら、ログオフを行ってからブラウザを終了してください。

①　サーバプロテクションサービス管理コンソールの右上にある[ログオフ]をクリックします。

②　サーバプロテクションサービス管理コンソールのログオン画面に戻ります。



3-3.ダッシュボード

ダッシュボードにはサーバプロテクションサービスで管理されているエージェントの情報が表示されます。

3-3-1.ダッシュボードの概要

ダッシュボードでは、サーバプロテクションサービスで管理されているエージェントで発生しているイベントの概要やシステムの情報を確認することができます。確認できる情報は以下の通りです。ただし、一部機能はサーバプロテクションサービスで提供しておりませんので、ご了承ください。

【サーバプロテクションサービスで提供している機能】

・アラートステータス
・アラート履歴
・コンピュータのステータス
・不正プログラム対策のステータス(コンピュータ)
・不正プログラム対策のステータス(不正プログラム)
・不正プログラム対策の保護ステータス
・不正プログラム対策イベント履歴
・不正プログラム検索のステータス
・Webレピュテーションの URLアクティビティ
・Webレピュテーションのコンピュータのアクティビティ
・Webレピュテーションイベント履歴
・IPS IPのアクティビティ(検出)
・IPS IPのアクティビティ(防御)
・IPSのアクティビティ(検出)
・IPSのアクティビティ(防御)
・IPSイベント履歴
・IPSコンピュータのアクティビティ(検出)
・IPSコンピュータのアクティビティ(防御)
・アプリケーションの種類のアクティビティ(検出)
・アプリケーションの種類のアクティビティ(防御)
・アプリケーションの種類のツリーマップ(検出)
・アプリケーションの種類のツリーマップ(防御)
・最新のIPSのアクティビティ(検出)
・最新のIPSのアクティビティ(防御)
・システムイベント履歴
・マイアカウントのステータス
・ログオン履歴
・セキュリティアップデートのステータス

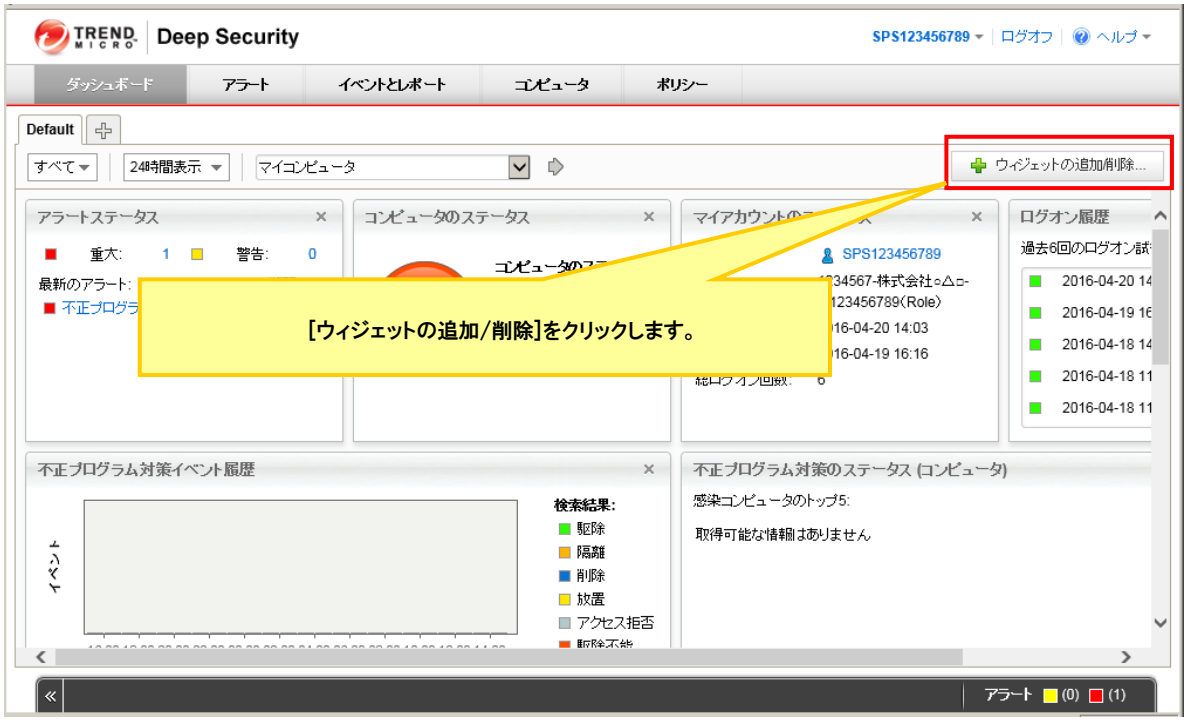
【サーバプロテクションサービスで提供していない機能】

・ファイアウォールIPのアクティビティ(検出)
・ファイアウォールIPのアクティビティ(防御)
・ファイアウォールのアクティビティ(検出)
・ファイアウォールのアクティビティ(防御)
・ファイアウォールイベント履歴
・ファイアウォールコンピュータのアクティビティ(検出)
・ファイアウォールコンピュータのアクティビティ(防御)
・ファイアウォールポートのアクティビティ(検出)
・ファイアウォールポートのアクティビティ(防御)
・攻撃の予兆検索のアクティビティ
・攻撃の予兆検索のコンピュータのアクティビティ
・攻撃の予兆検索履歴
・Managerノードのステータス
・アクティビティ概要
・ソフトウェアアップデート

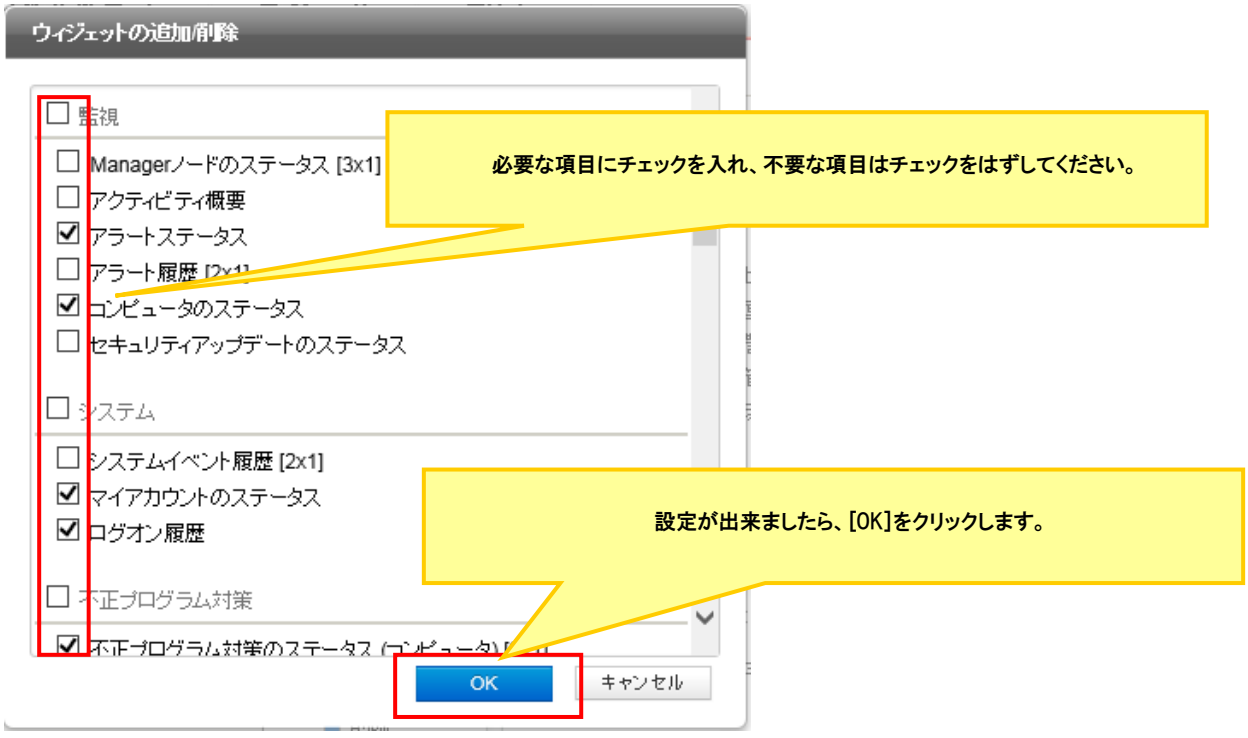
3-3-2.ウィジェットの追加/削除

ダッシュボードのウィジェットを追加、削除し、必要な情報を閲覧できるようにします。

① サーバプロテクションサービスのポータルサイトトップページを開きます。



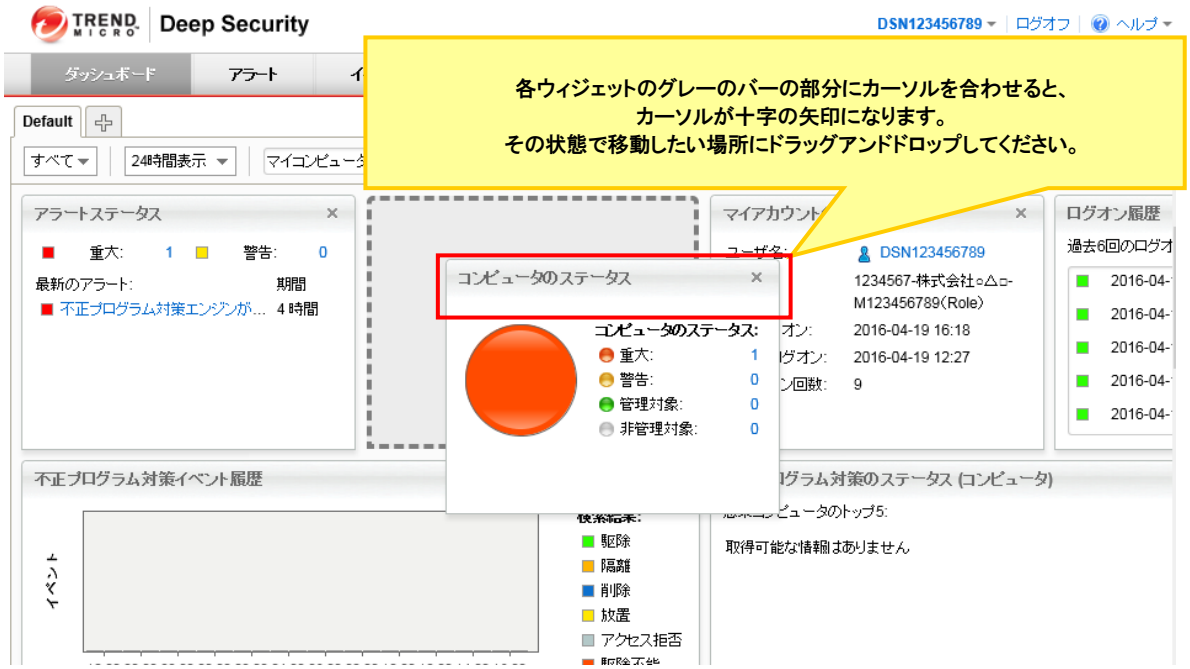
② ウィジェットの追加/削除の画面が開きます。



③ ダッシュボードで設定が反映されたことをご確認ください。

3-3-3.ウィジェットの配置変更

① サーバプロテクションサービス管理コンソールが開き、ダッシュボード画面を表示します。

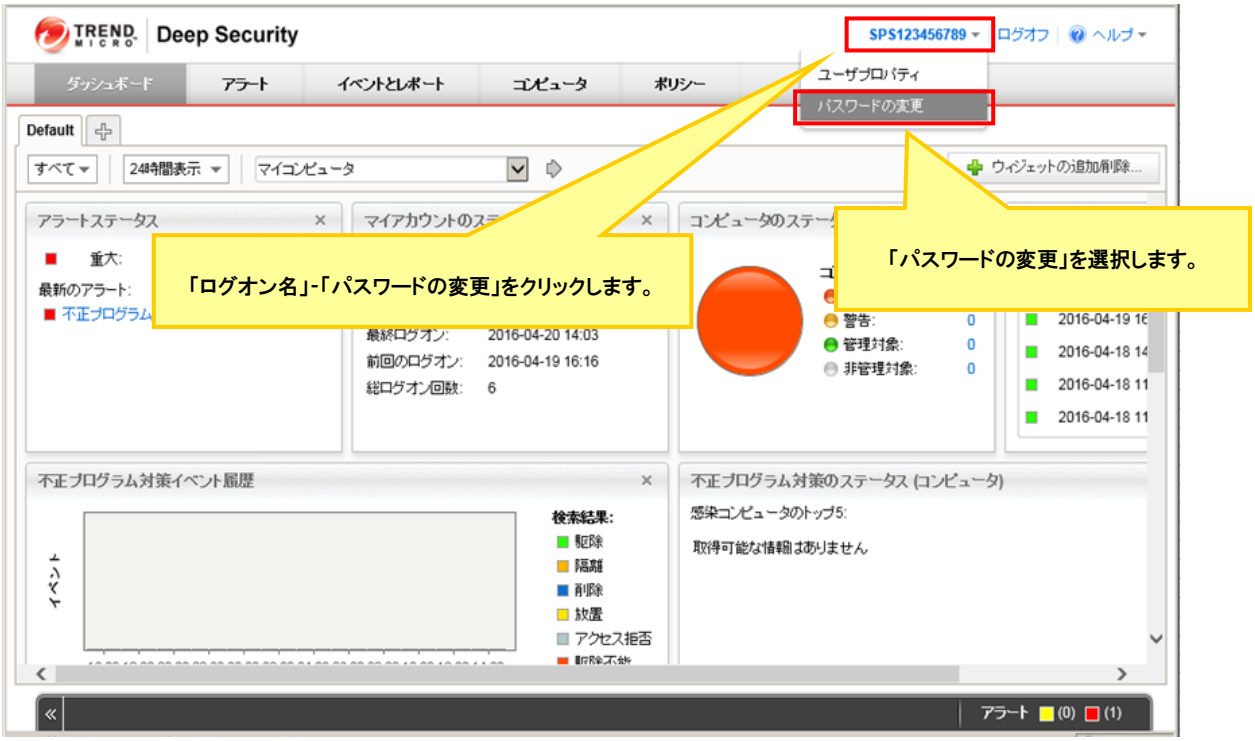


② ウィジェットが移動します。

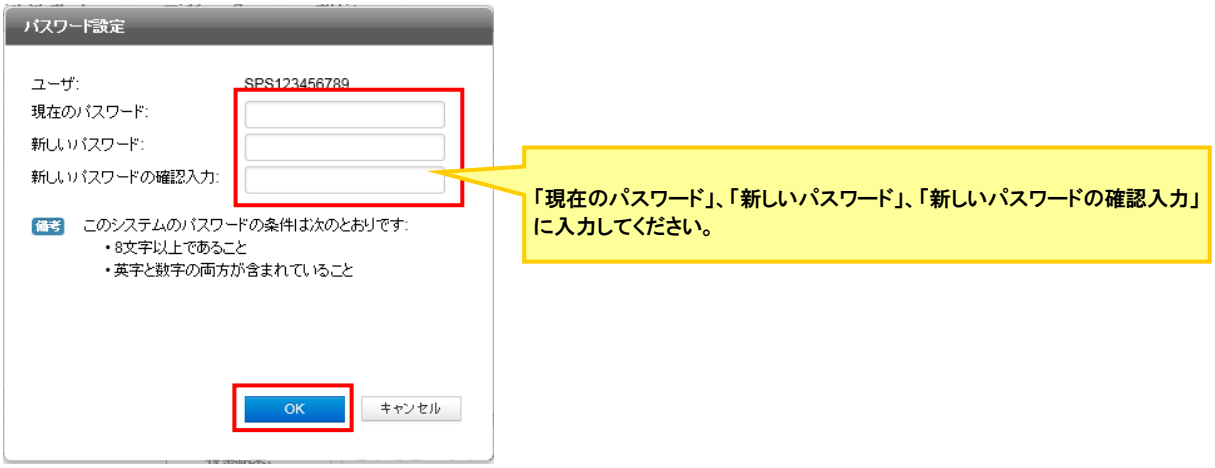
3-3-4.パスワードの変更

「サーバプロテクションサービス登録完了のお知らせ」に記載されているパスワードは初期パスワードとなっておりますので、お客様にて変更をお願いいたします。また、発行後のパスワードに関してはお客様管理とさせていただきますのでお忘れにならないようお願いいたします。

① サーバプロテクションサービスの管理コンソールにログオンします。



② 現在のパスワード・新しいパスワード/確認入力にそれぞれ入力をします。



! 重要 パスワードの条件

8文字以上でかつ英字と数字の両方が含まれている必要があります。

3-4.アラート、ログの参照

管理コンソールから各エージェントの状態を確認します。運用時に確認するべき項目は以下のとおりです。最低でも週に一度、定期的に確認を行うようにしてください。

- アラート
- 不正プログラム対策イベント
- 侵入防御イベント
- Webレピュテーションイベント

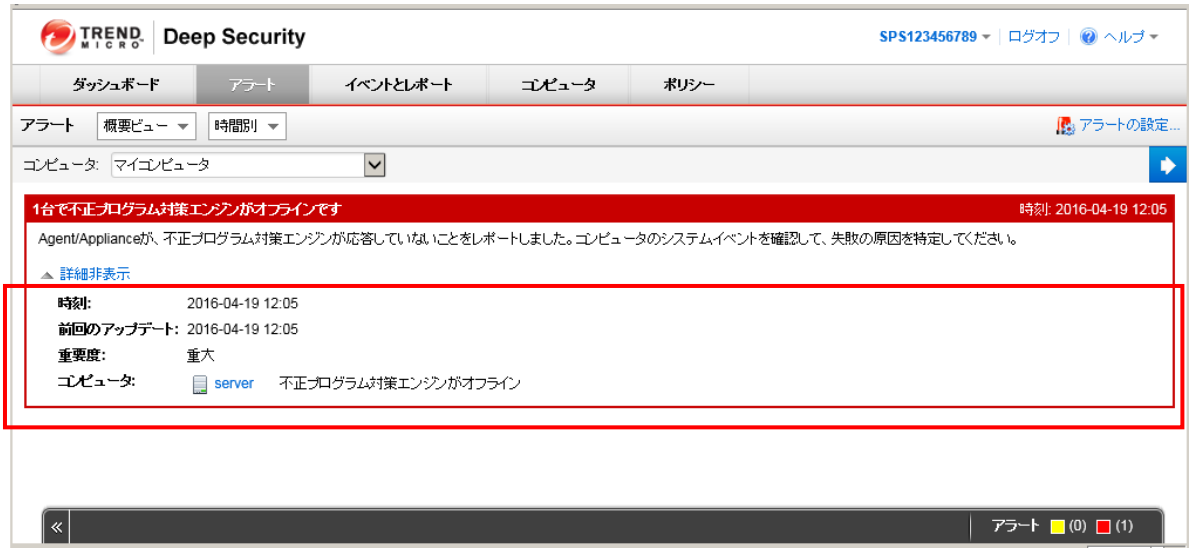
3-4-1.アラートの参照

管理コンソールの[アラート]からエージェントで発生しているアラートを確認します。
アラートとは、各エージェントでパターンファイルが更新されていない、検索エンジンがオフラインになっている等、何らかの問題が発生した場合に、管理コンソール上に通知を出す機能です。

① サーバプロテクションサービスの管理コンソールにログオンします。

② アラートの画面が表示されます。

③　アラートの詳細が表示されますので、内容をご確認ください。



MEMO　主なアラートの種類

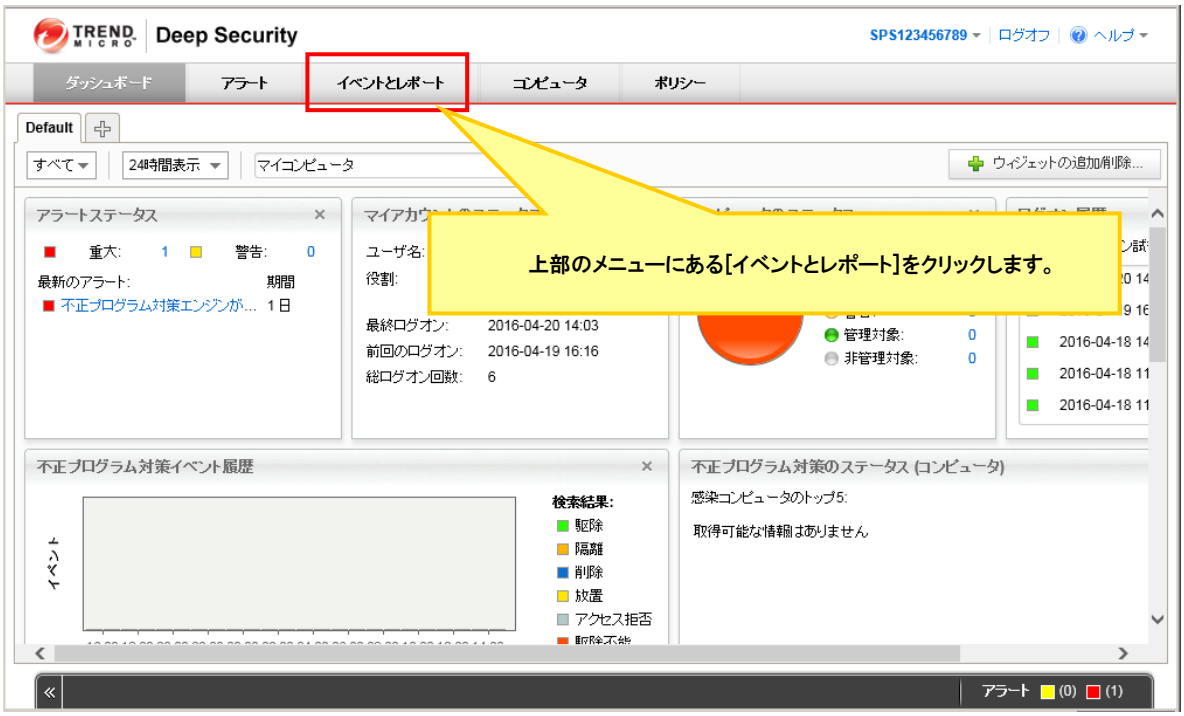
主なアラートには以下のような種類があります。

アラート名	重要度	内容
侵入防御エンジンがオフライン	重大	侵入防御エンジンが認識できません。
Relayアップデートサービスを利用不可	重大	アップデートサーバに接続できません。この場合、トレンドマイクロ社のアップデートサーバからアップデートを行います。
Webレピュテーションイベントアラート	警告	エージェントでWebレピュテーションのポリシー違反等のイベントが発生しています。
不正プログラム対策コンポーネントのアップデートの失敗	重大	ウイルスパターンファイル等、コンポーネントのアップデートに失敗しています。
コンピュータがアップデートを受信していない	警告	サーバプロテクションサービスのサーバから各エージェントに出されたアップデートの通知を、エージェントが受信していません。
コンピュータの再起動が必要	警告	エージェントがインストールされている端末でOS再起動が必要です。
不正プログラム対策アラート	警告	ウイルスが検出されています。
不正プログラム対策エンジンがオフライン	重大	不正プログラム対策エンジンが認識できません。
新しいパターンファイルアップデートがダウンロード済みで利用可能	警告	サーバプロテクションサービスのサーバが新しいパターンファイルまたはエンジンを取得し、利用可能な状態になっています。

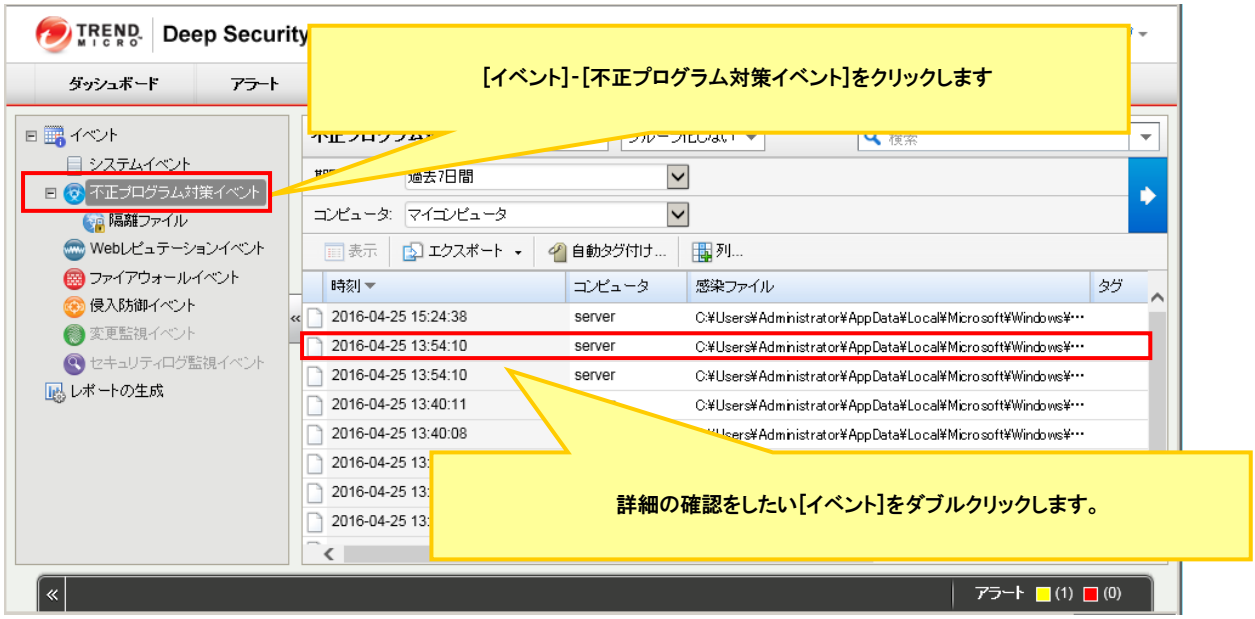
3-4-2.不正プログラム対策イベントの参照

管理コンソールの[不正プログラム対策イベント]から各エージェントでウイルス感染していないかを確認します。[不正プログラム対策イベント]とは、ウイルスやスパイウェアに感染した際に発生するイベントです。

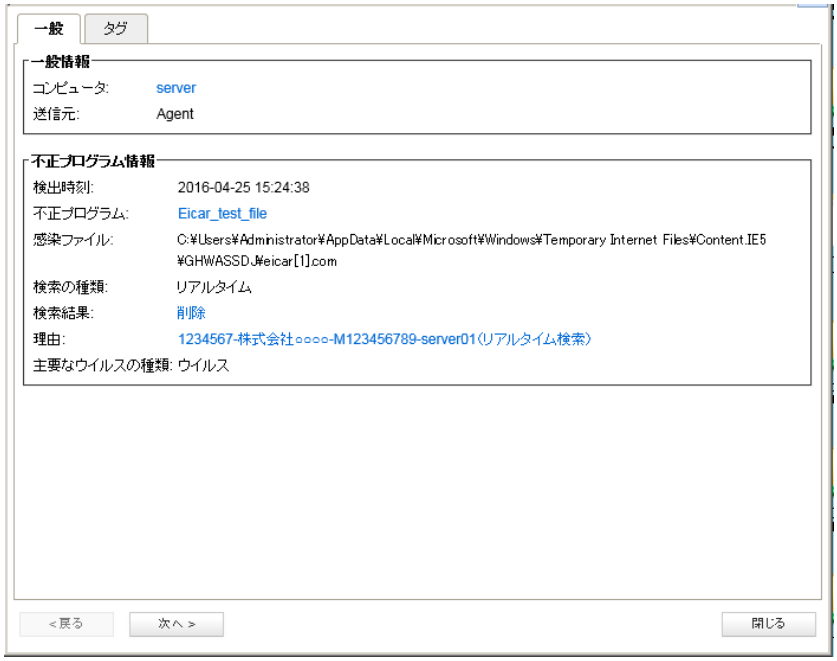
① サーバプロテクションサービスの管理コンソールにログオンします。



② 不正プログラム対策イベントの画面が表示されます。



③　イベントの詳細が表示されますので、内容をご確認の上、適宜ご対応ください。



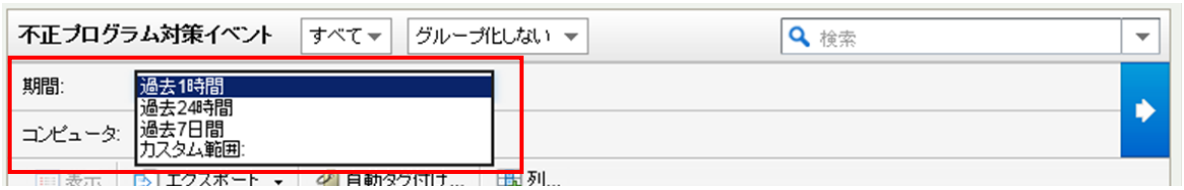
MEMO　ウイルス感染時の対処方法

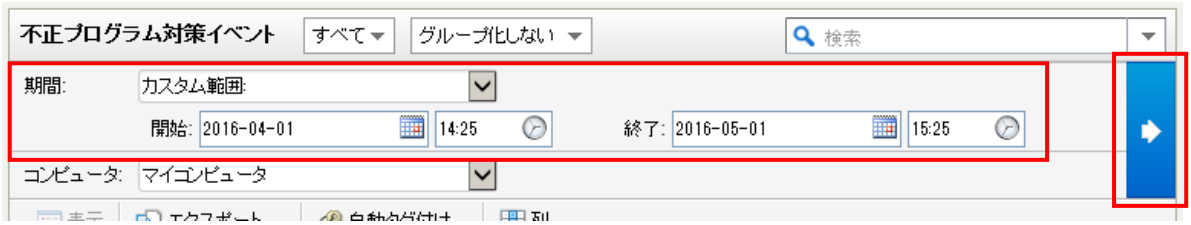
「検索結果」に表示される処理が「駆除」、「削除」、「隔離」以外の場合、別途ウイルスの処理を行う必要があります。

参照 5.ウイルス感染時の対処方法

ヒント　不正プログラム対策イベントを表示する期間の指定

不正プログラム対策イベントは、初期値では過去1時間のイベント表示する設定になっています。期間は「過去1時間」、「過去24時間」、「過去7日間」と、「カスタム範囲」があります。カスタム範囲を選択した場合は、開始と終了の日時を設定し、右側にある矢印をクリックします。

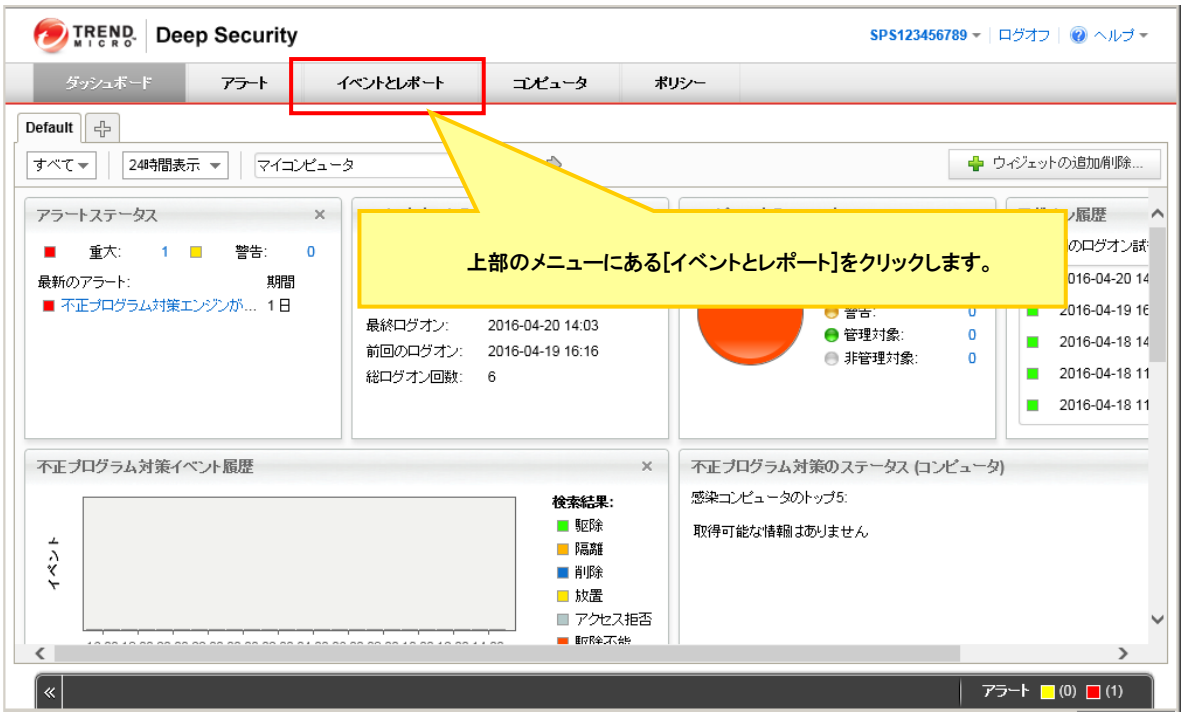




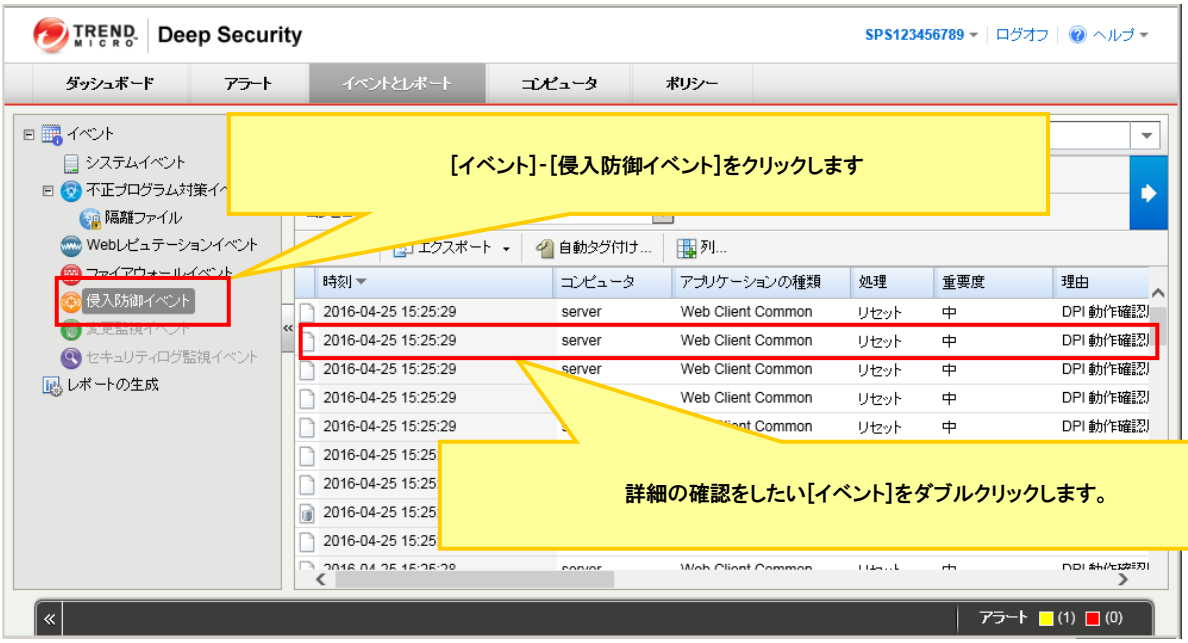
3-4-3.侵入防御(仮想パッチ)イベントの参照

管理コンソールの[侵入防御イベント]から各エージェントで仮想パッチに関連するイベントが発生していないかを確認します。[侵入防御イベント]とは、推奨スキャンで適用された仮想パッチに対して攻撃が行われた場合に発生するイベントです。

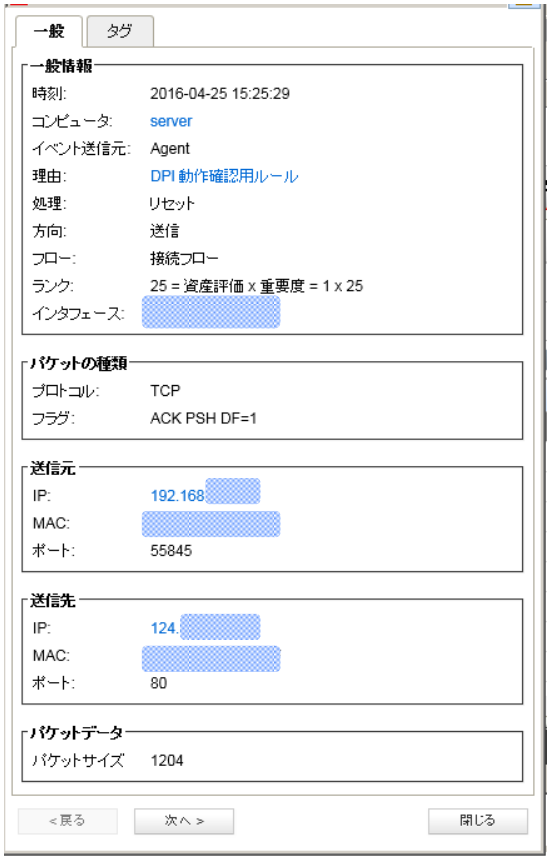
① サーバプロテクションサービスの管理コンソールにログオンします。



② 侵入防御イベントの画面が表示されます。



③　イベントの詳細が表示されますので、内容をご確認ください。

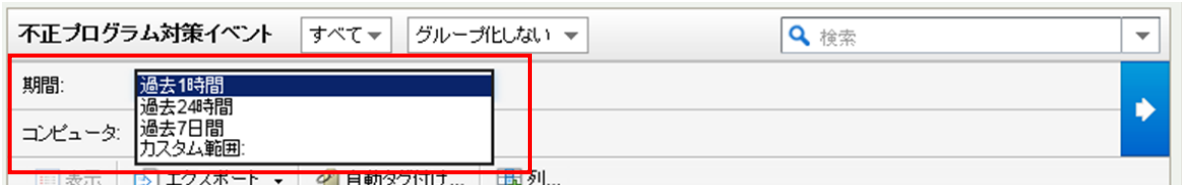


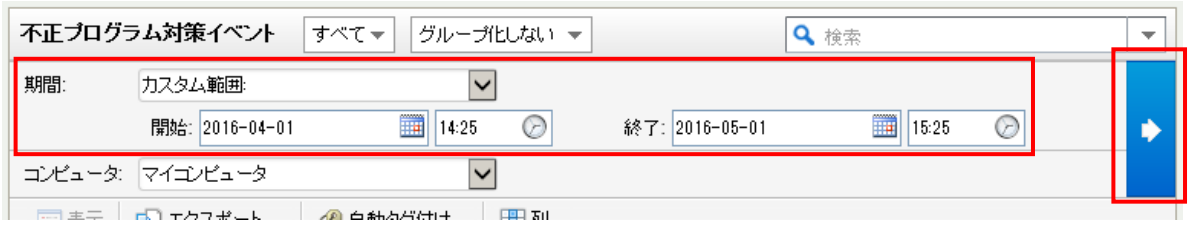
MEMO　侵入防御イベント発生時の対処方法

特定の端末に侵入防御イベントが大量に発生している場合は、外部から攻撃を受けている可能性があります。弊社エンジニアまでご相談ください。

ヒント　侵入防御イベントを表示する期間の指定

侵入防御イベントは、初期値では過去1時間のイベント表示する設定になっています。期間は「過去1時間」、「過去24時間」、「過去7日間」と、「カスタム範囲」があります。カスタム範囲を選択した場合は、開始と終了の日時を設定し、右側にある矢印をクリックします。

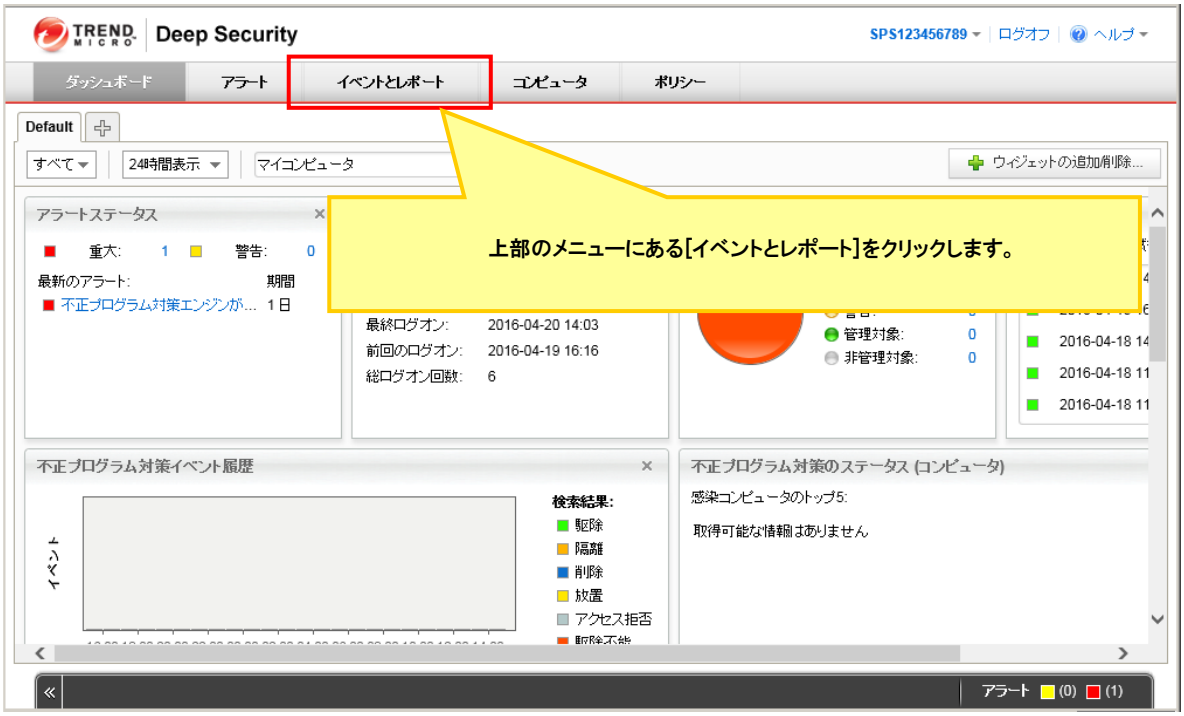




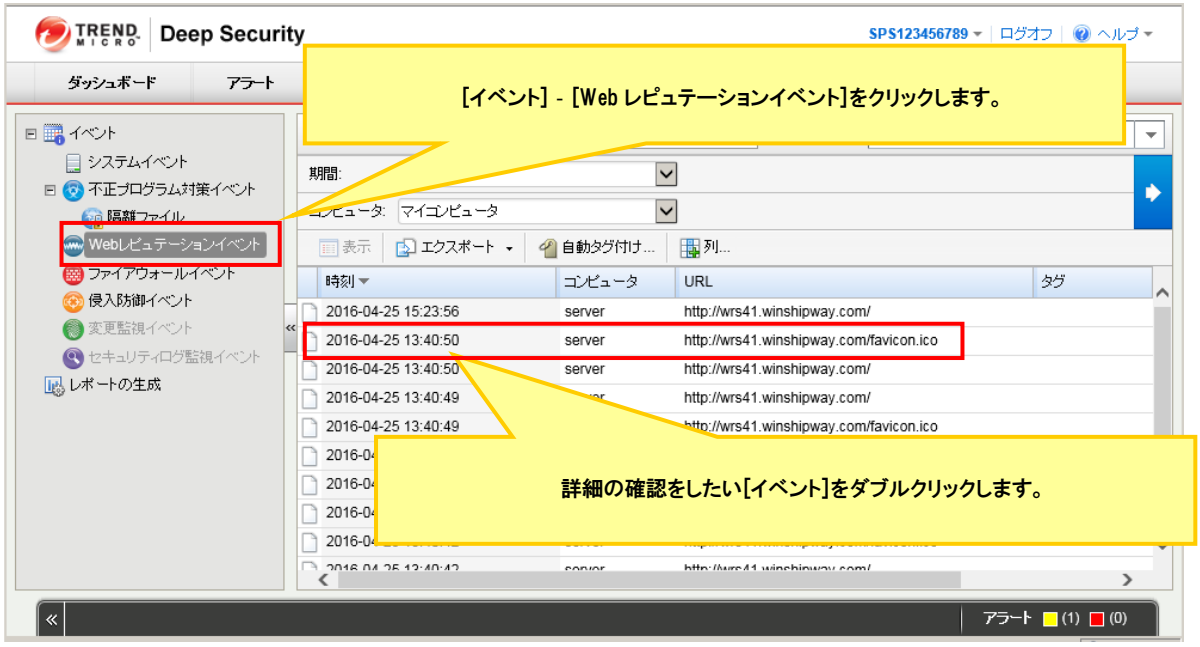
3-4-4.Webレピュテーションイベントの参照

管理コンソールの[Webレピュテーションイベント]から各エージェントでウイルス感染する危険のあるWebサイトに接続していないかを確認します。

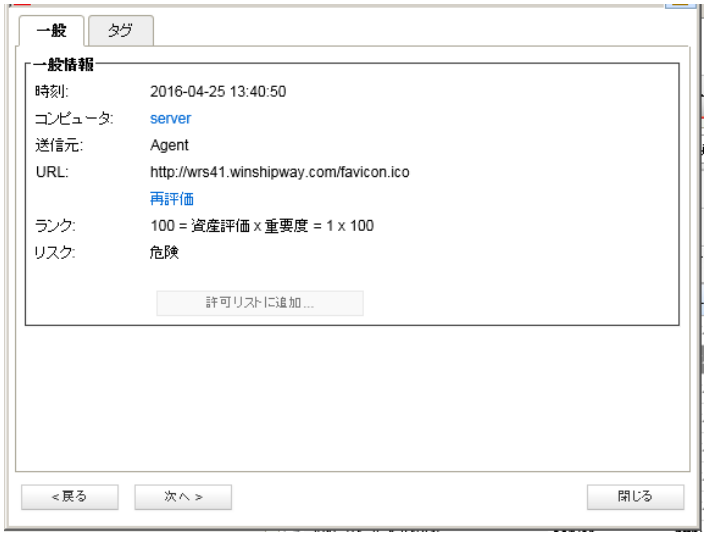
① サーバプロテクションサービスの管理コンソールにログオンします。



② Webレピュテーションイベントの画面が表示されます。



③　イベントの詳細が表示されますので、内容をご確認ください。

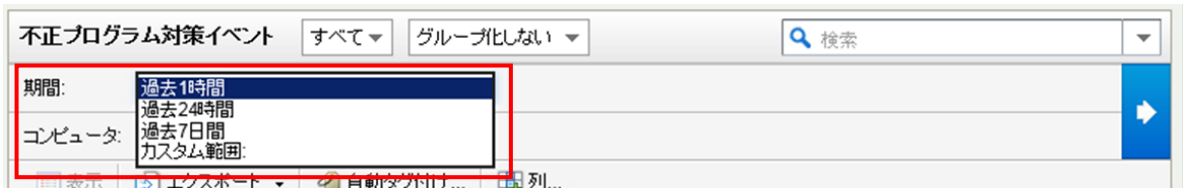


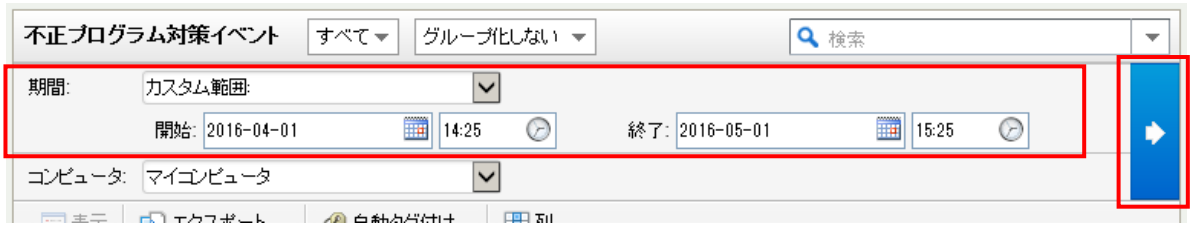
MEMO　Webレピュテーションイベントの対処方法

特定の端末でエンドユーザ様に覚えのないWebサイトへのアクセスがブロックされたイベントが発生している場合は、その端末がウイルス感染している可能性があります。調査をご要望の場合は弊社担当エンジニアまでご連絡ください。

ヒント　Webレピュテーションイベントを表示する期間の指定

Webレピュテーションイベントは、初期値では過去1時間のイベント表示する設定になっています。期間は「過去1時間」、「過去24時間」、「過去7日間」と、「カスタム範囲」があります。カスタム範囲を選択した場合は、開始と終了の日時を設定し、右側にある矢印をクリックします。



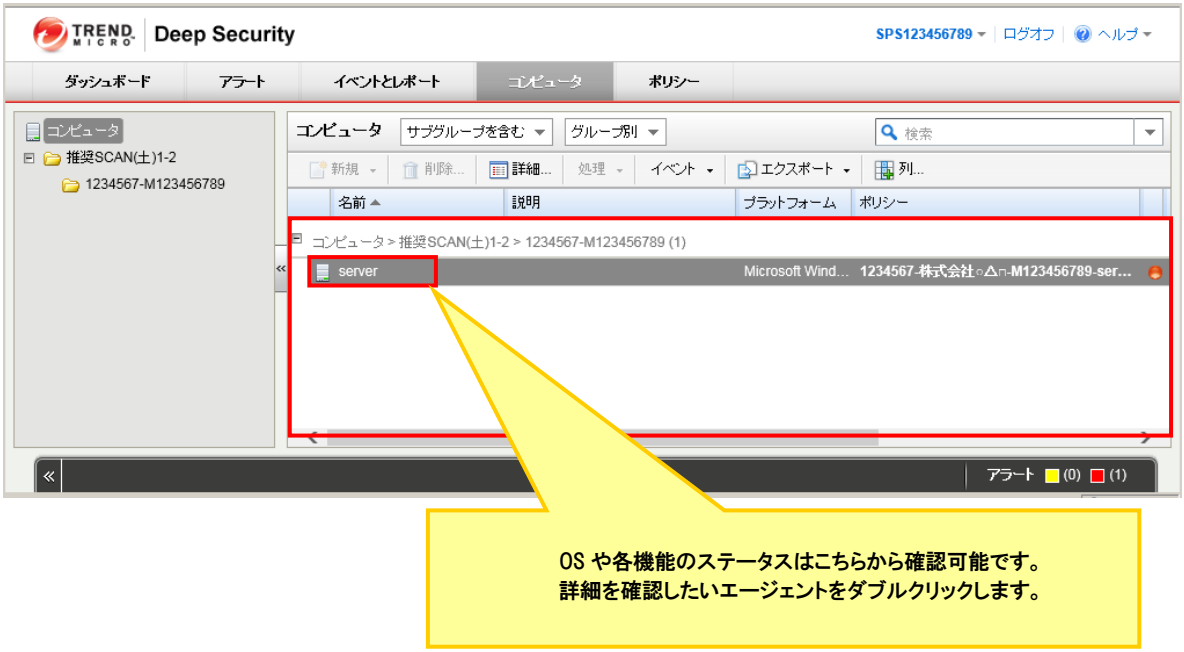


3-5. サーバ情報の参照

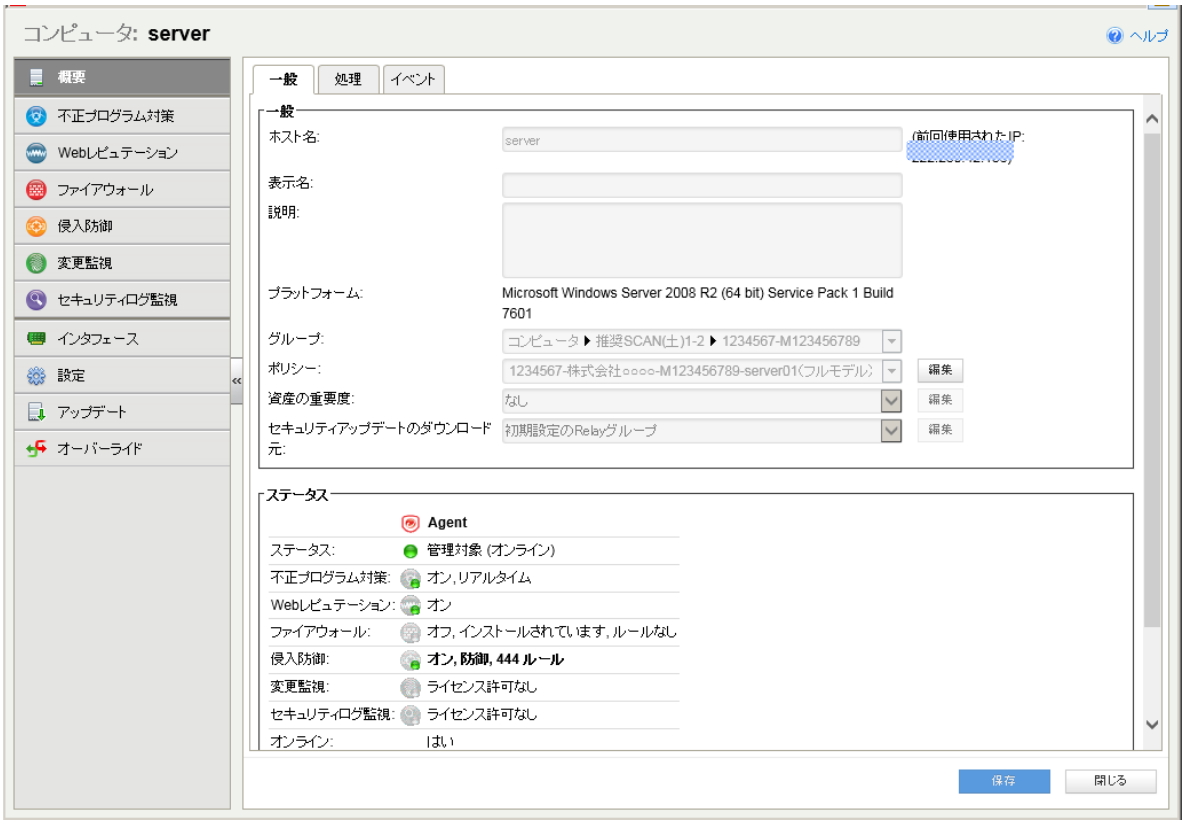
エージェントになっているサーバOSの情報を管理コンソールから参照することができます。

① サーバプロテクションサービスの管理コンソールにログオンします。

② サーバプロテクションサービスで管理されているエージェントが表示されます。OSや各機能のステータスはこちらから確認可能です。



③ サーバ情報の詳細が表示されます。



項目名	アイコン	状態	意味
ステータス		管理対象(オンライン)	サーバプロテクションサービスの管理対象で、管理サーバとオンライン状態です。正常時はこちらの状態になります。
		管理対象(オフライン)	サーバプロテクションサービスの管理対象で、管理サーバとオフライン状態です。 ※オフラインであってもアイコンの状態はオンラインと同じです。必ず状態の表記をご確認ください。
不正プログラム対策		オン、リアルタイム	不正プログラム対策がオンの状態です。 サーバプロテクションサービスの「フルモデル」または「ウイルス対策モデル」をご契約戴いたお客様はこの状態になります。
		オフ、インストールされていません	不正プログラム対策がオフの状態です。 サーバプロテクションサービスの「仮想パッチモデル」をご契約戴いたお客様はこの状態になります。
Webレピュテーション		オン	Webレピュテーションがオンの状態です。 サーバプロテクションサービスの「フルモデル」または「ウイルス対策モデル」をご契約戴いたお客様はこの状態になります。
		オフ、インストールされていません	Webレピュテーションがオフ状態です。 サーバプロテクションサービスの「仮想パッチモデル」をご契約戴いたお客様はこの状態になります。
侵入防御		防御、XXルール	侵入防御がオンの状態で、XXは有効なルール数を表しています。 サーバプロテクションサービスの「フルモデル」または「仮想パッチモデル」をご契約戴いたお客様はこの状態になります。
		オフ、インストールされていません	侵入防御がオフの状態です。 サーバプロテクションサービスの「ウイルス対策モデル」をご契約戴いたお客様はこの状態になります。

※ファイアウォール機能はサーバプロテクションサービスでは提供しておりません。

表示は「オフ，インストールされています，ルールなし」で問題ありません。

3-6. レポート

管理コンソールから生成できるレポートについてご説明します。

サーバプロテクションサービスの管理コンソールから確認いただける主なレポートの種類は以下の通りです。

レポートはPDF形式かリッチテキスト方式のいずれかで生成することができます。

なお、レポートの対象とすることができる期間は、レポート生成時から過去4週間分の情報のみとなりますので、ご了承ください。

レポート名	説明
アラートレポート	指定した期間中のアラートを「頻度別の種類」、「時系列」でレポートします。
不正プログラム対策レポート	指定した期間中の「不正プログラムに感染したコンピュータのトップ25」、「不正プログラムのトップ25」、「未完了の予約検索」をレポートします。
コンピュータレポート	「コンピュータのステータス」、「OSの種類」、「前回のアップデート」情報などがレポートされます。
侵入防御レポート	指定した期間中の「侵入防御イベントの履歴(防御モード、検出モード)」、各モード毎の「イベントトップ25」「送信元IPトップ25」、「アプリケーション種類のトップ25」をレポートします。
推奨設定レポート	推奨スキャンにより推奨設定された「アプリケーションの種類」や「侵入防御ルール」をレポートします。
概要レポート	指定した期間中の「アラートのトップ5」、「感染のトップ5」、「Webレピュテーションのトップ5」およびアラートレポート、不正プログラム対策レポート、Webレピュテーションレポートなどの簡易情報をまとめてレポートします。
Webレピュテーションレポート	指定した期間中の「Webレピュテーションイベントのトップ25」、「URLのトップ25」をレポートします。

ヒント レポート生成の条件

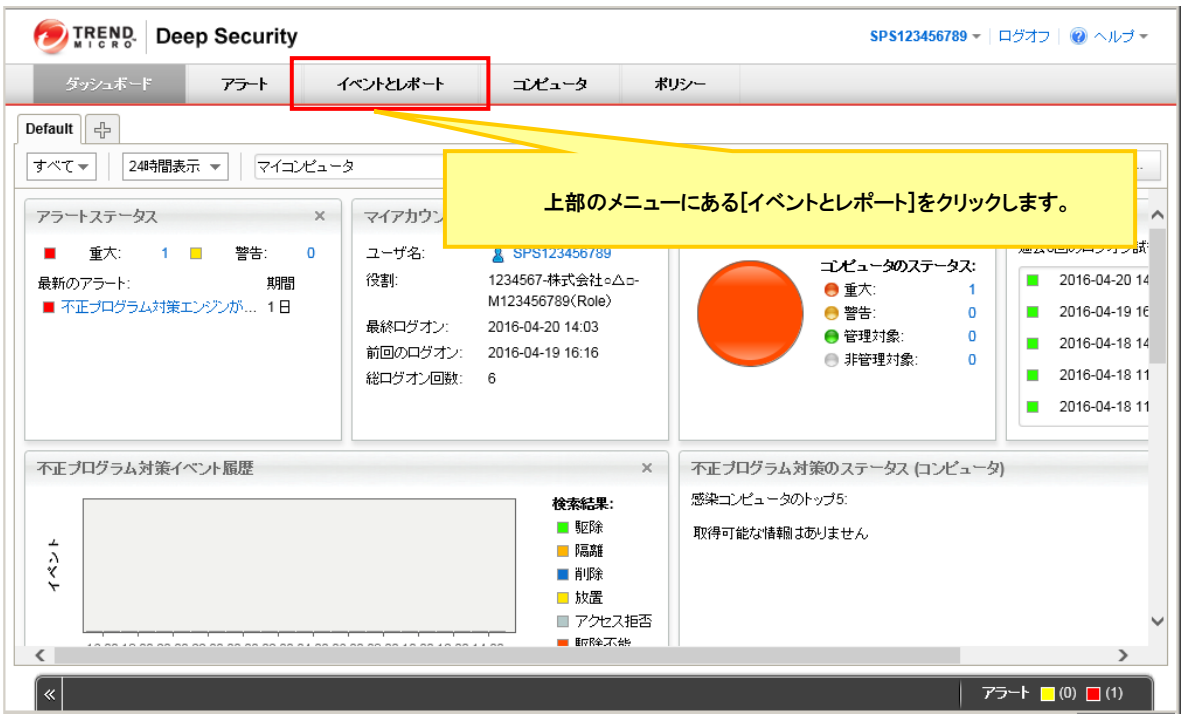
レポートを生成する際、条件を設定することが可能です。レポートによって、設定できる条件とできない条件があります。
詳細は以下の一覧をご確認ください。

【主なレポートの条件】

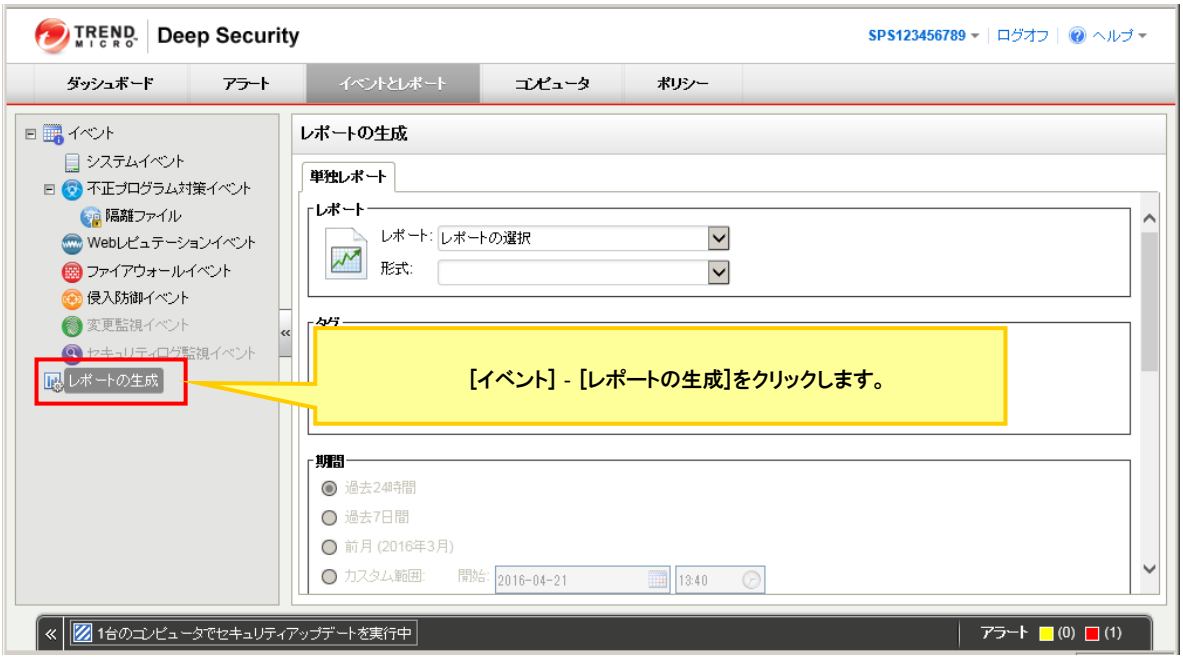
レポート名	形式	期間	コンピュータ	暗号化
アラートレポート	PDF または リッチテキスト	・過去24時間 ・過去7日間 ・カスタム範囲	・マイコンピュータ ・グループ内のコンピュータ ・セキュリティプロファイルを使用しているコンピュータ ・コンピュータ名指定	―
不正プログラム対策レポート		・過去24時間 ・過去7日間 ・カスタム範囲		―
コンピュータレポート		―		―
侵入防御レポート		・過去24時間 ・過去7日間 ・カスタム範囲		―
推奨設定レポート		―		―
概要レポート		・過去24時間 ・過去7日間 ・カスタム範囲		―
Webレピュテーションレポート		・過去24時間 ・過去7日間 ・カスタム範囲		―

3-6-1.レポート作成方法

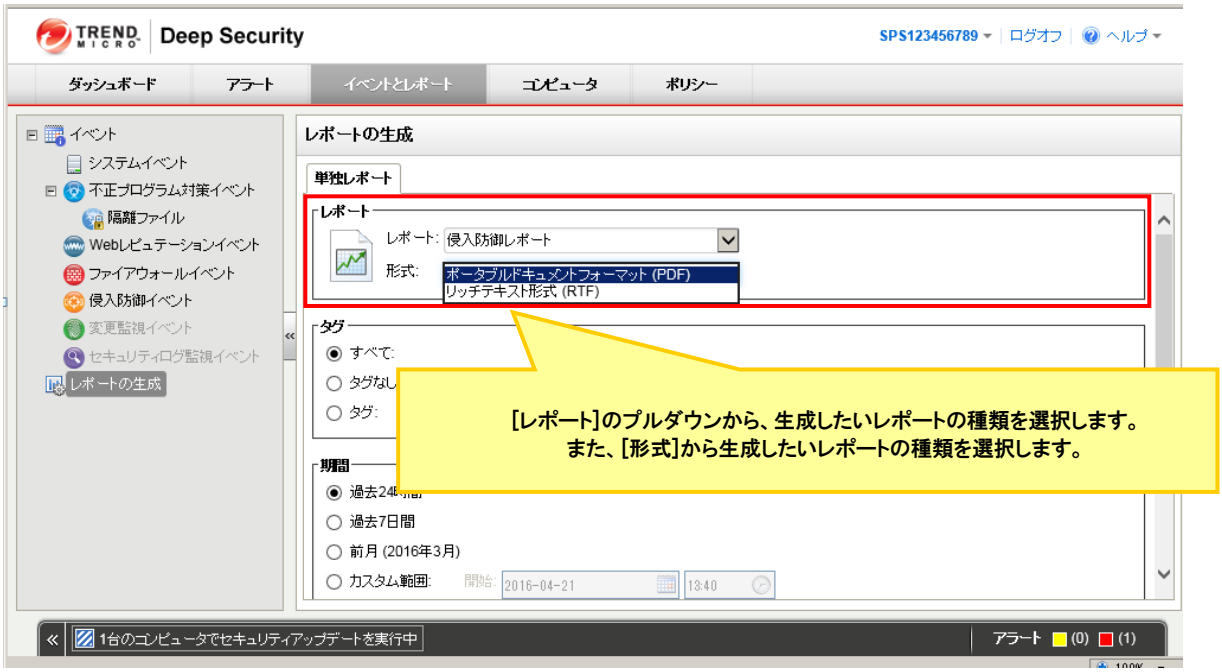
① サーバプロテクションサービスの管理コンソールにログオンします。



② レポートの画面が表示されます。



③　レポートの形式を選択します。

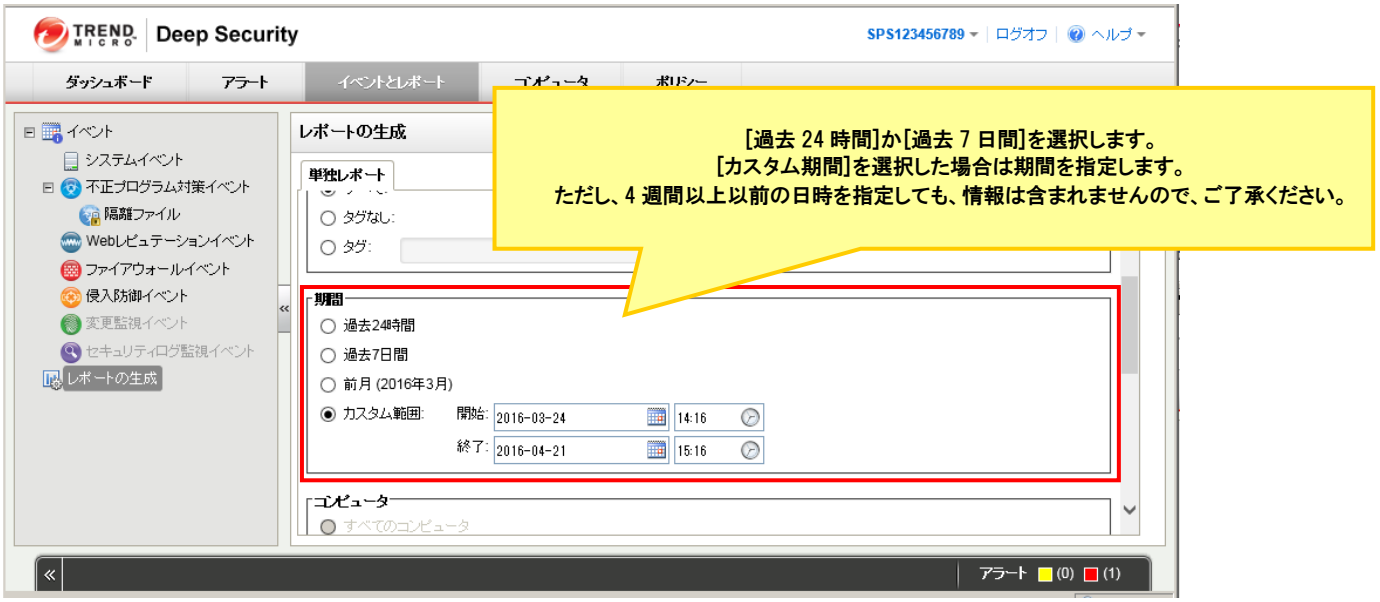


④　タグの設定をします。

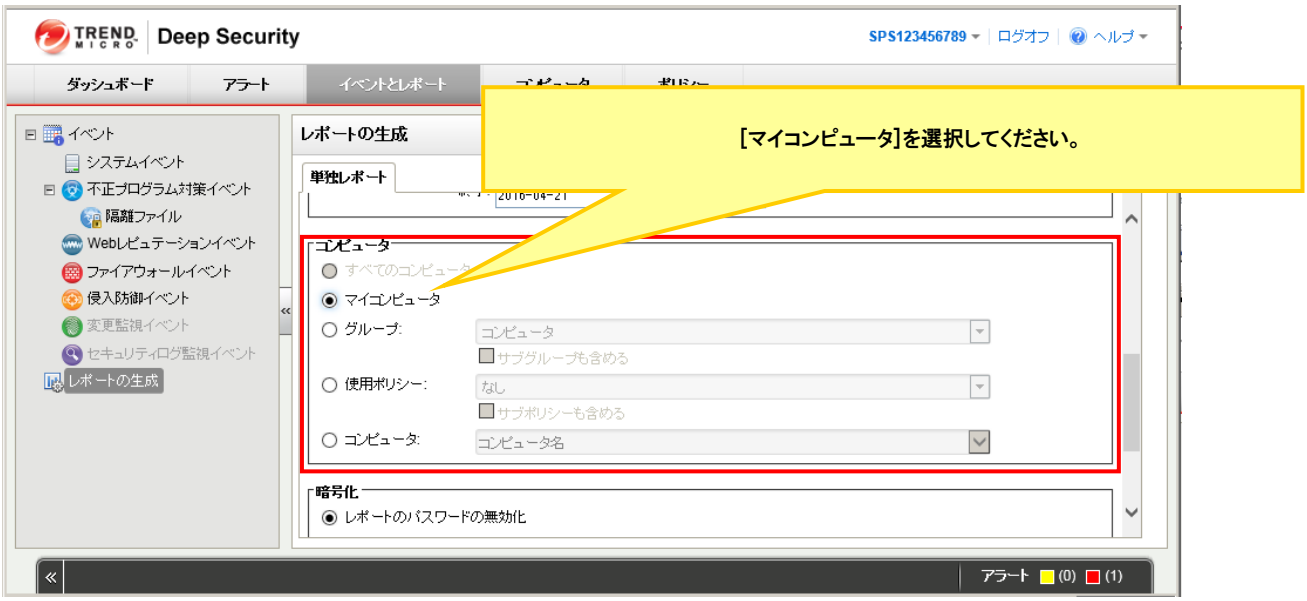
ヒント　タグ

イベントデータを含むレポートを選択する場合、イベントタグでレポートをフィルタするオプションを使用できます。[すべて]は全てのイベント、[タグなし]はタグ付けされていないイベントを対象とします。また、[タグ]を選択して1つ以上のタグを指定すると、指定したタグを含むイベントのみをレポートに含めることができます。　※本サービスではタグはご利用できません。

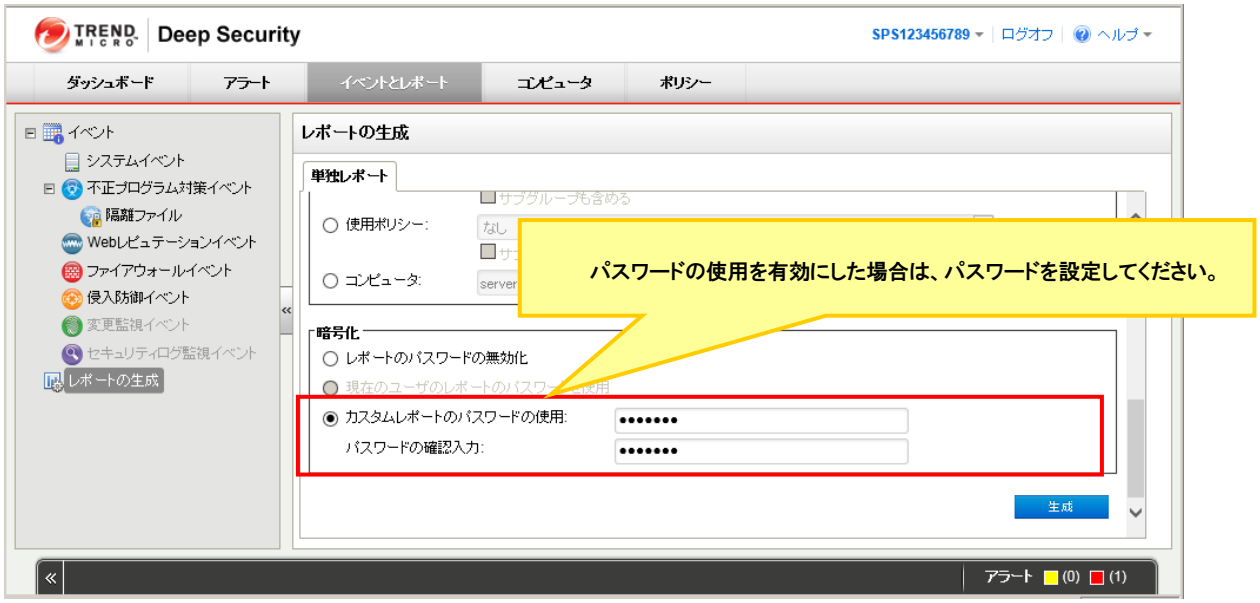
⑤　期間を指定します。



⑥　コンピュータを指定します。

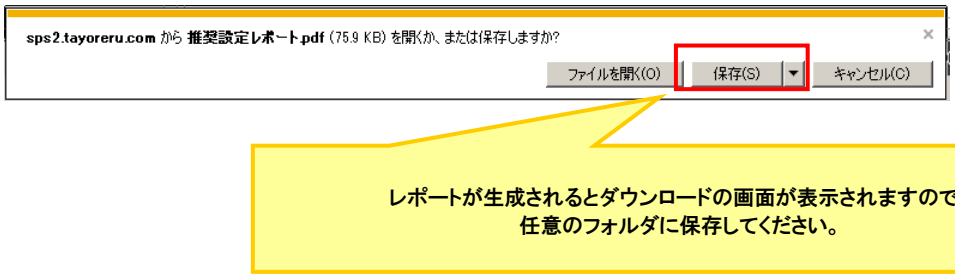


⑦　暗号化の設定をします。



⑧　設定が終わったら、レポートを生成します。

⑨　レポートが生成されます。

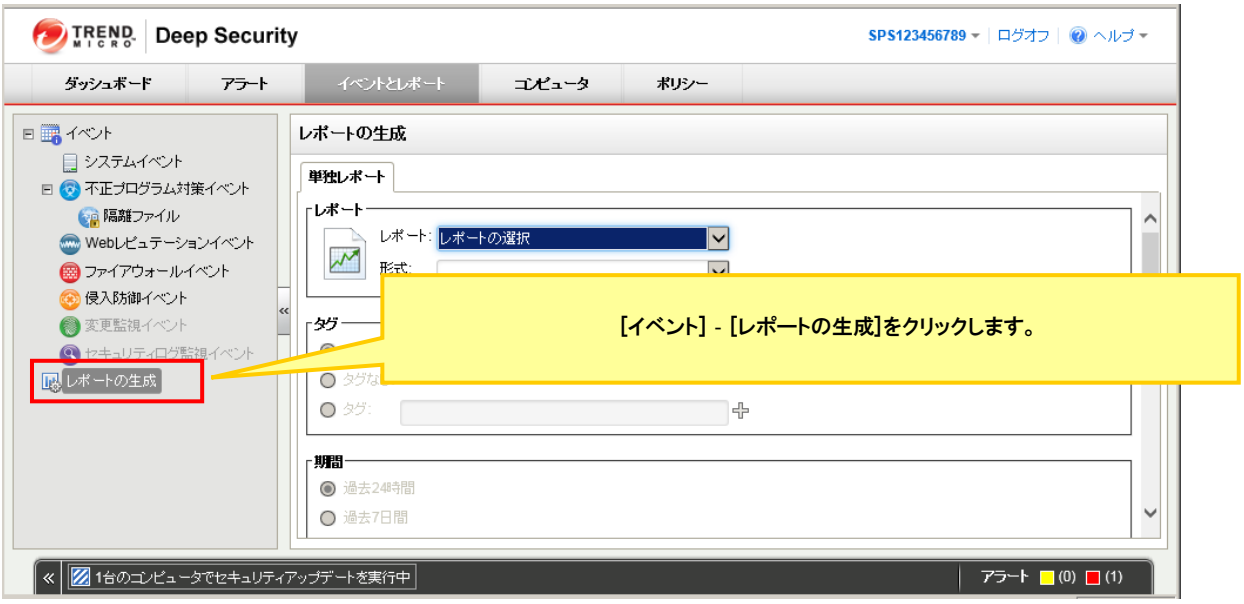


3-6-2.(例)ウイルスレポート

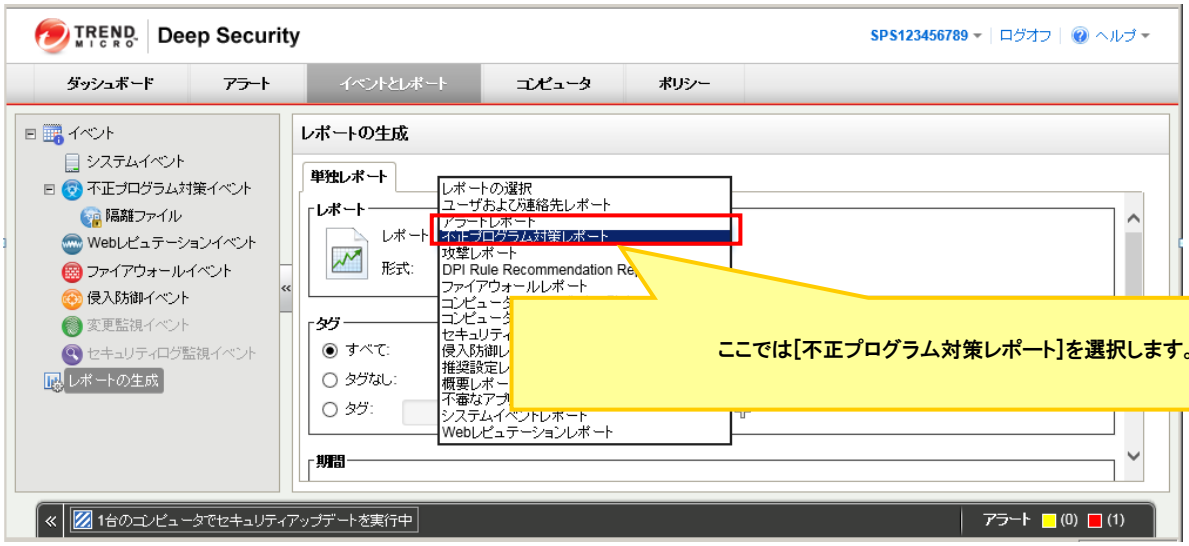
例として、不正プログラム対策レポートの生成手順を記載いたします。

① サーバプロテクションサービスの管理コンソールにログオンします。

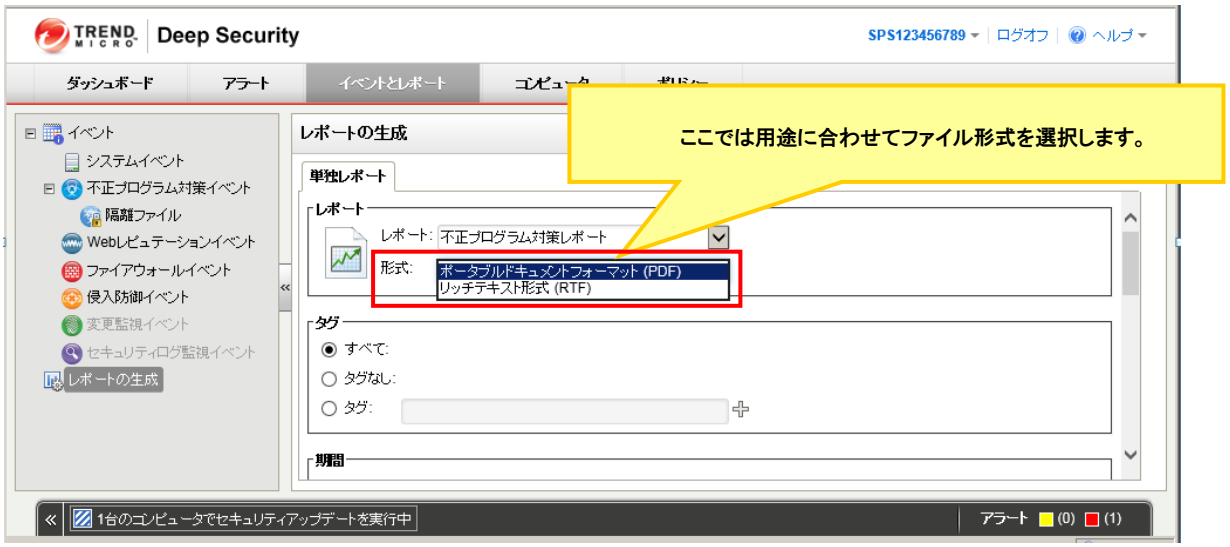
② レポートの画面が表示されます。



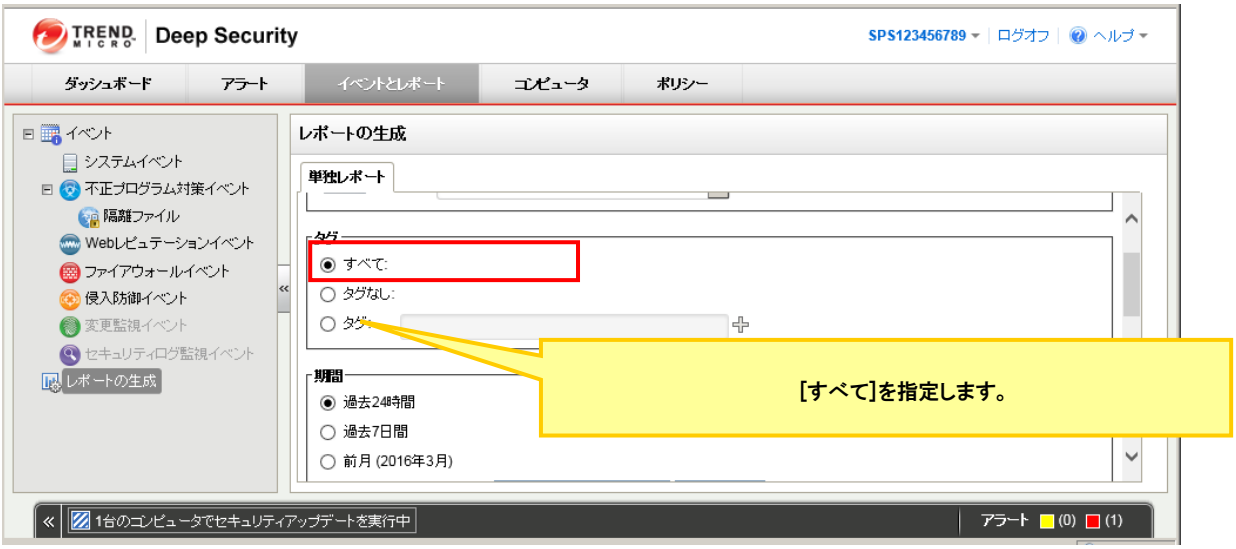
③　レポートの形式を選択します。



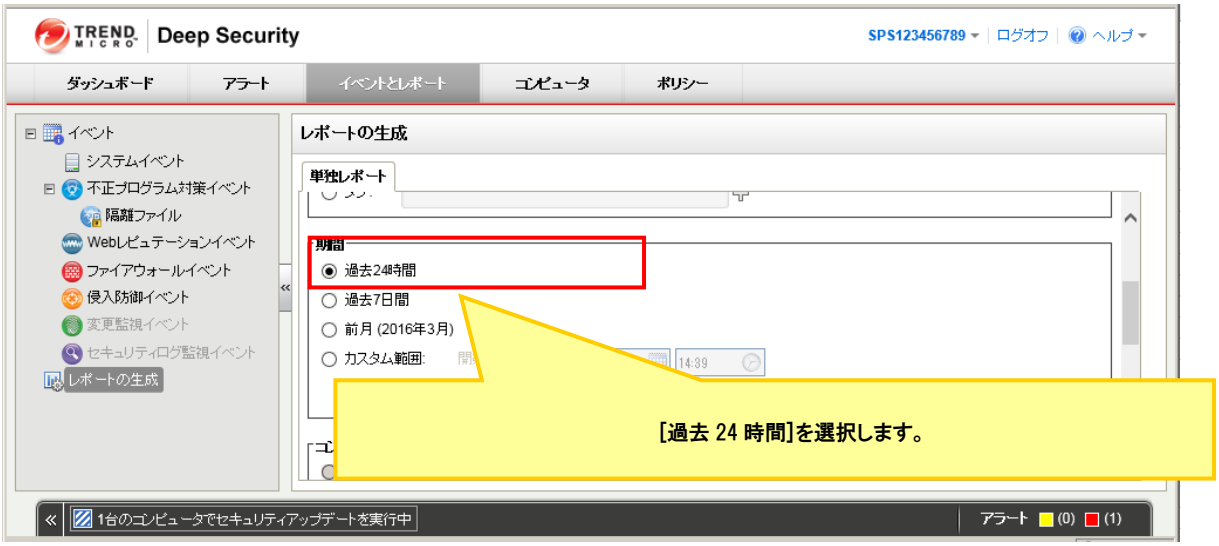
④　レポートのファイル形式を選択します。



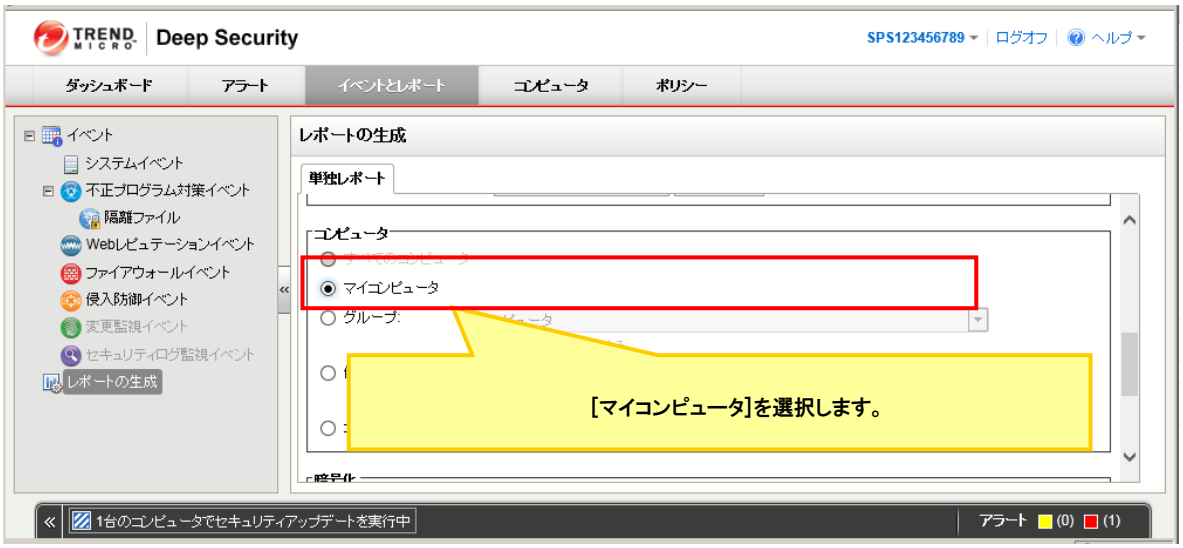
⑤　タグの設定をします。



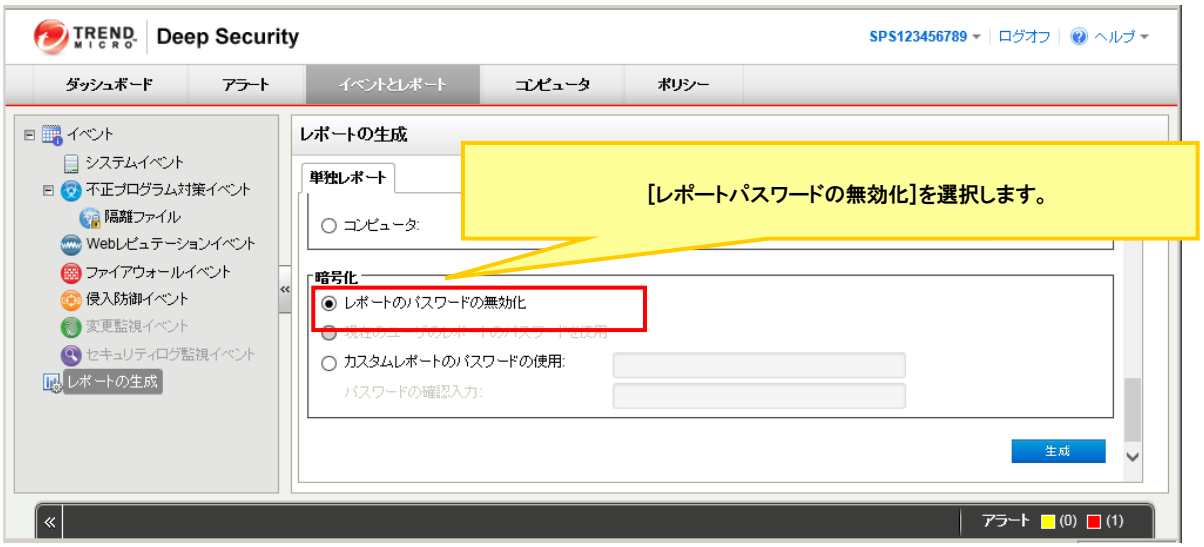
⑥　期間を指定します。



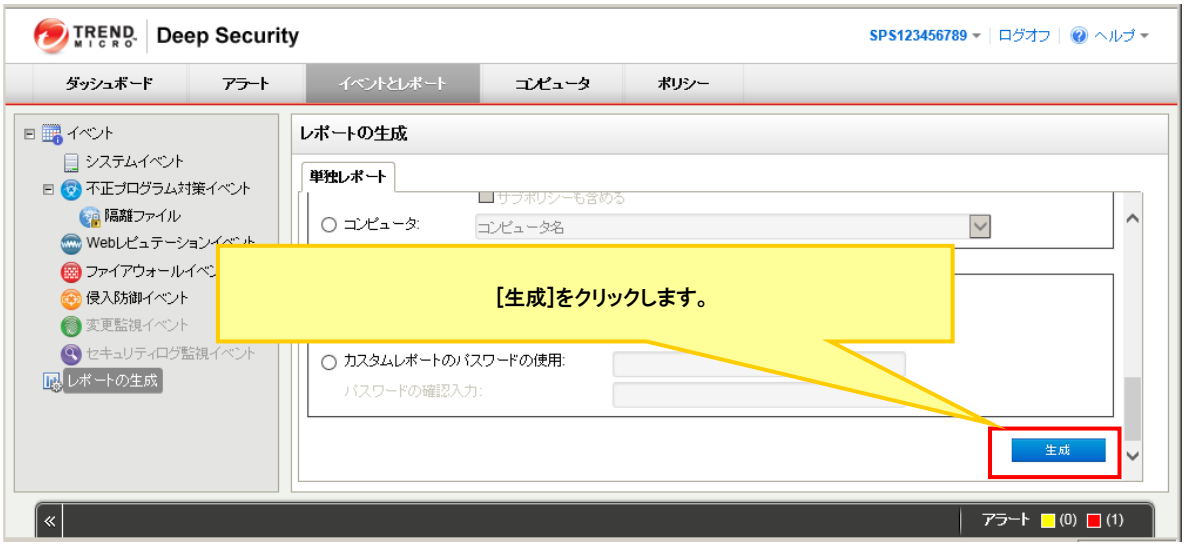
⑦　コンピュータを指定します。



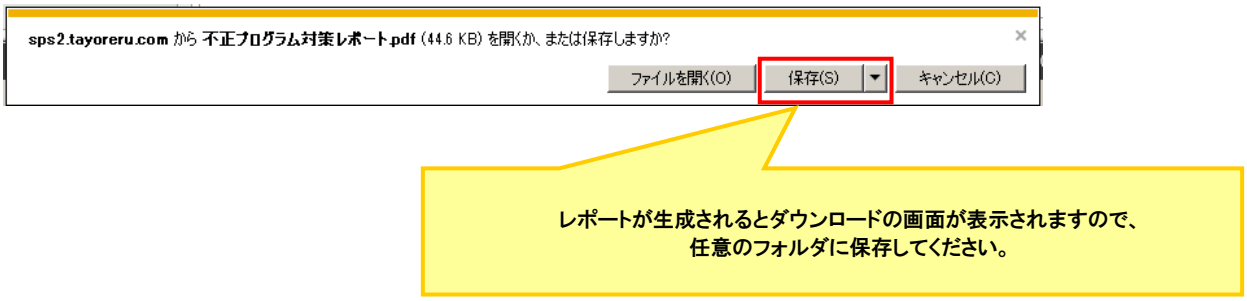
⑧　暗号化の設定をします。



⑨　設定が終わったら、レポートを生成します。



⑩　レポートが生成されます。

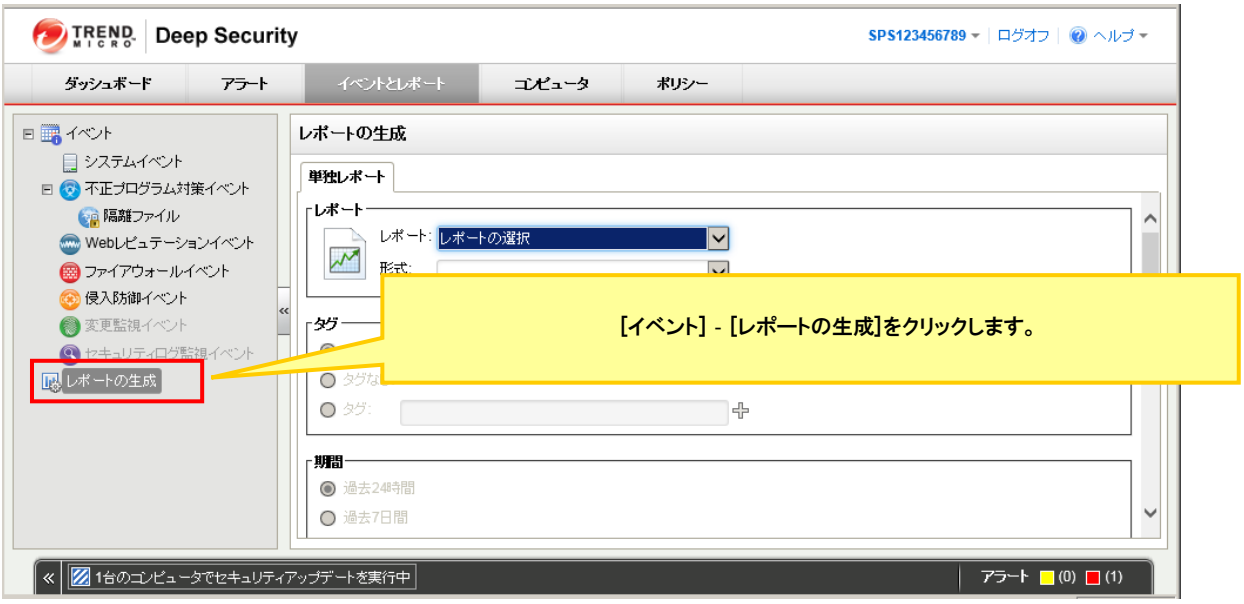


3-6-3.(例)侵入防御レポート

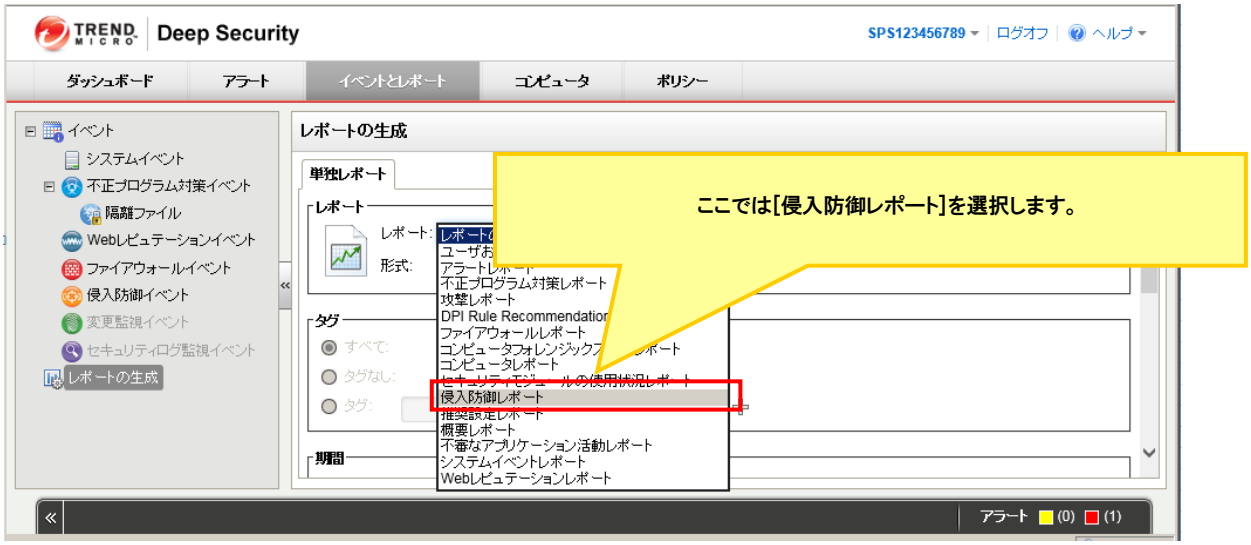
例として、仮想パッチのレポートである侵入防御レポートの生成手順を記載いたします。

① サーバプロテクションサービスの管理コンソールにログオンします。

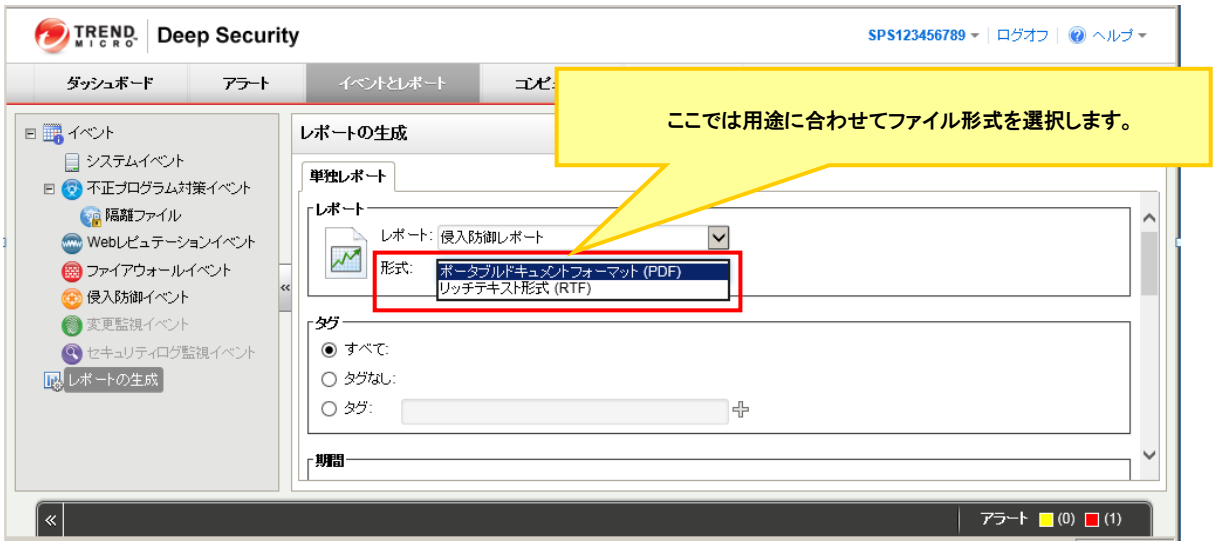
② レポートの画面が表示されます。



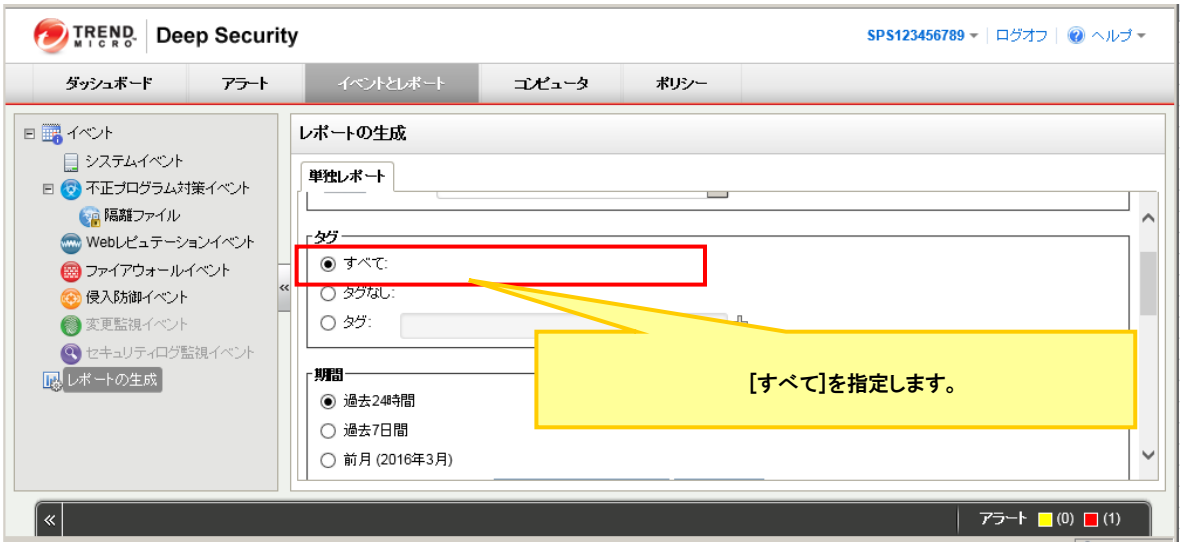
③　レポートの形式を選択します。



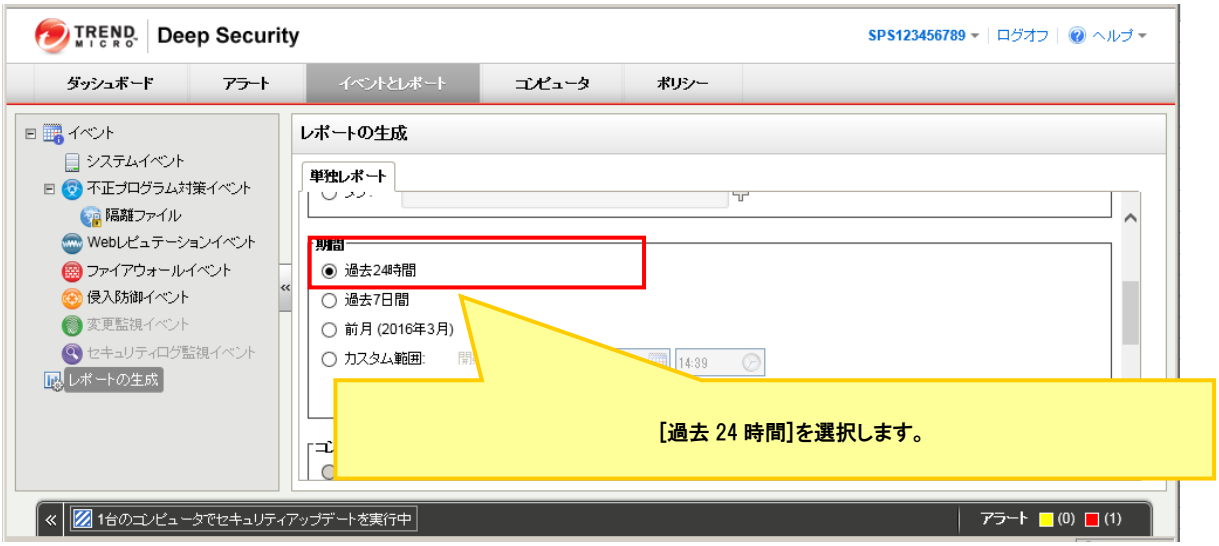
④　レポートのファイル形式を選択します。



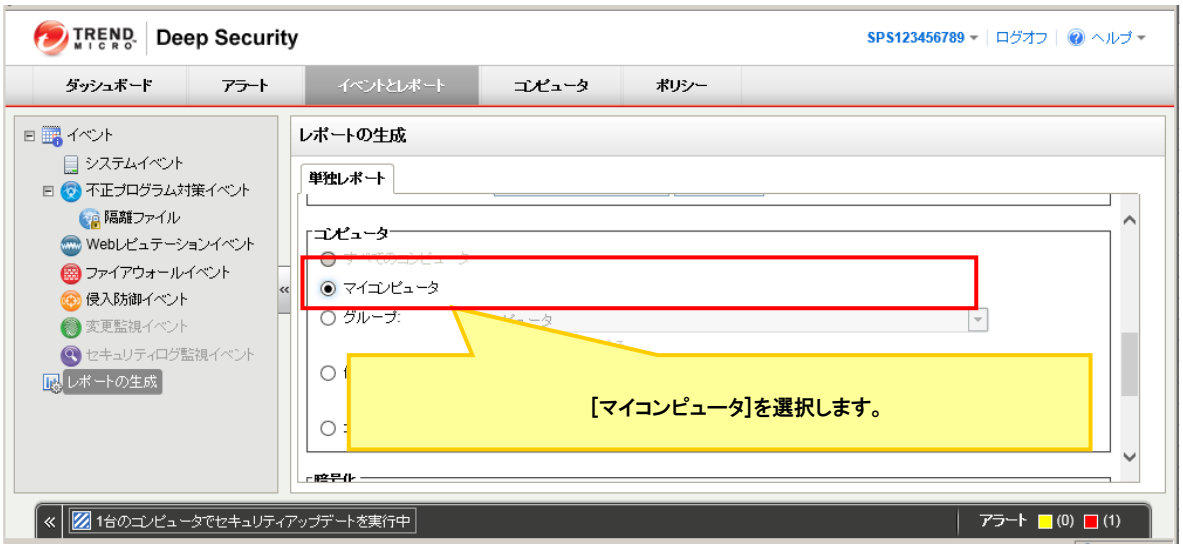
⑤　タグの設定をします。



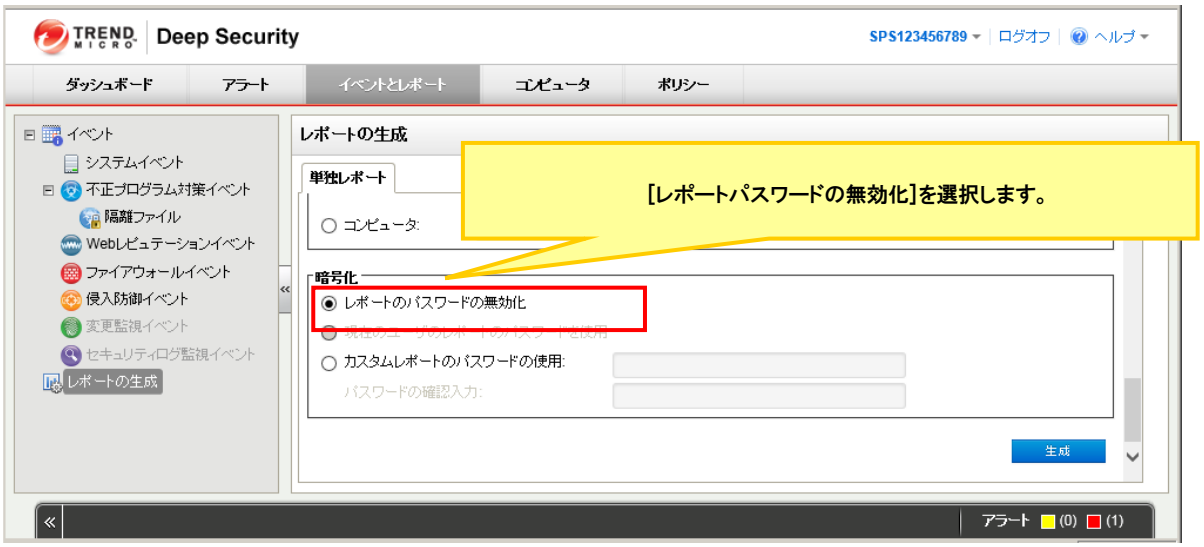
⑥　期間を指定します。



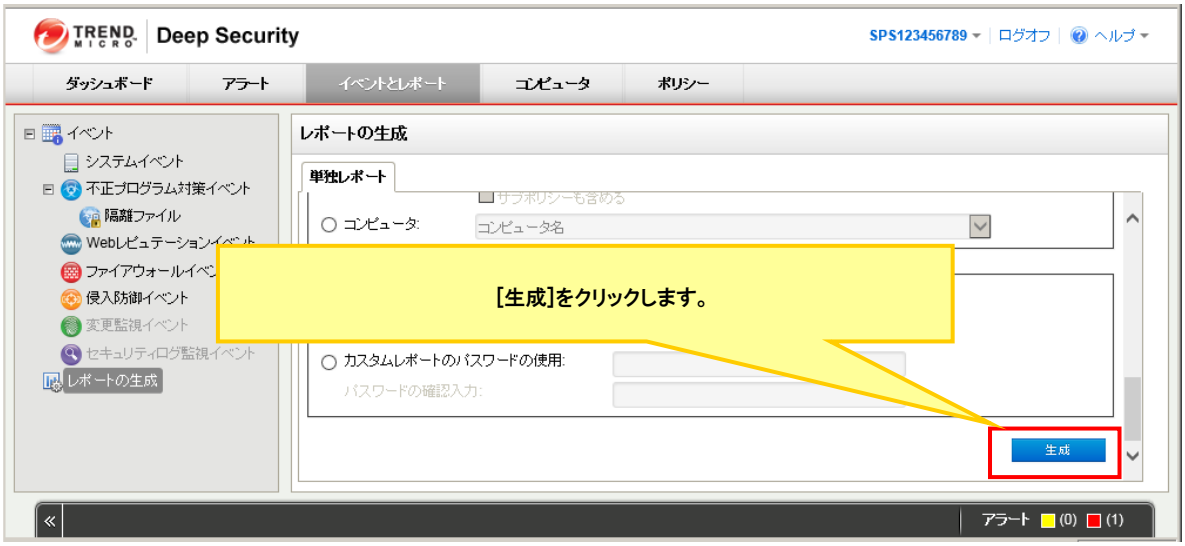
⑦　コンピュータを指定します。



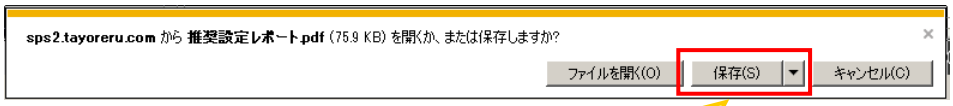
⑧　暗号化の設定をします。



⑨　設定が終わったら、レポートを生成します。



⑩　レポートが生成されます。



レポートが生成されるとダウンロードの画面が表示されますので、
任意のフォルダに保存してください。

4.タスクトレイアイコンについて

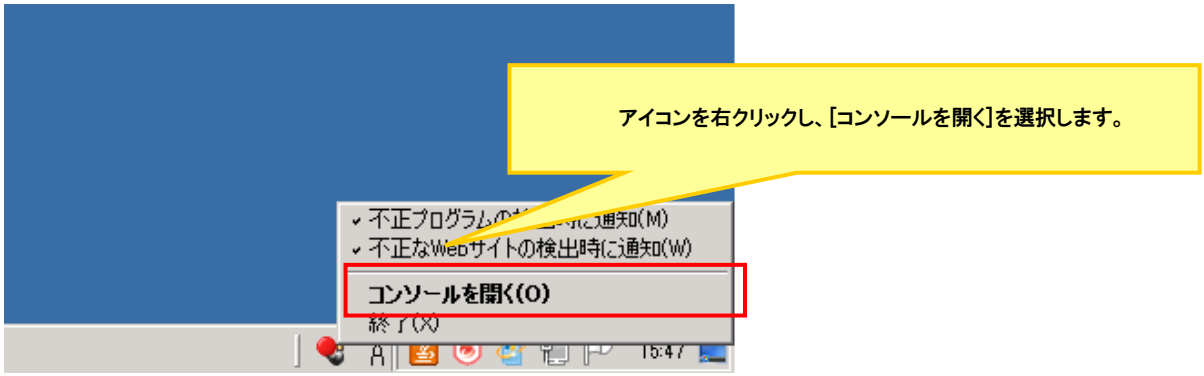
この章では、エージェントのタスクトレイアイコンについて説明します。
エージェント側でサーバプロテクションサービスのイベントを確認する場合、タスクトレイアイコンからクライアント用のコンソールを使用します。

4-1.イベントの参照

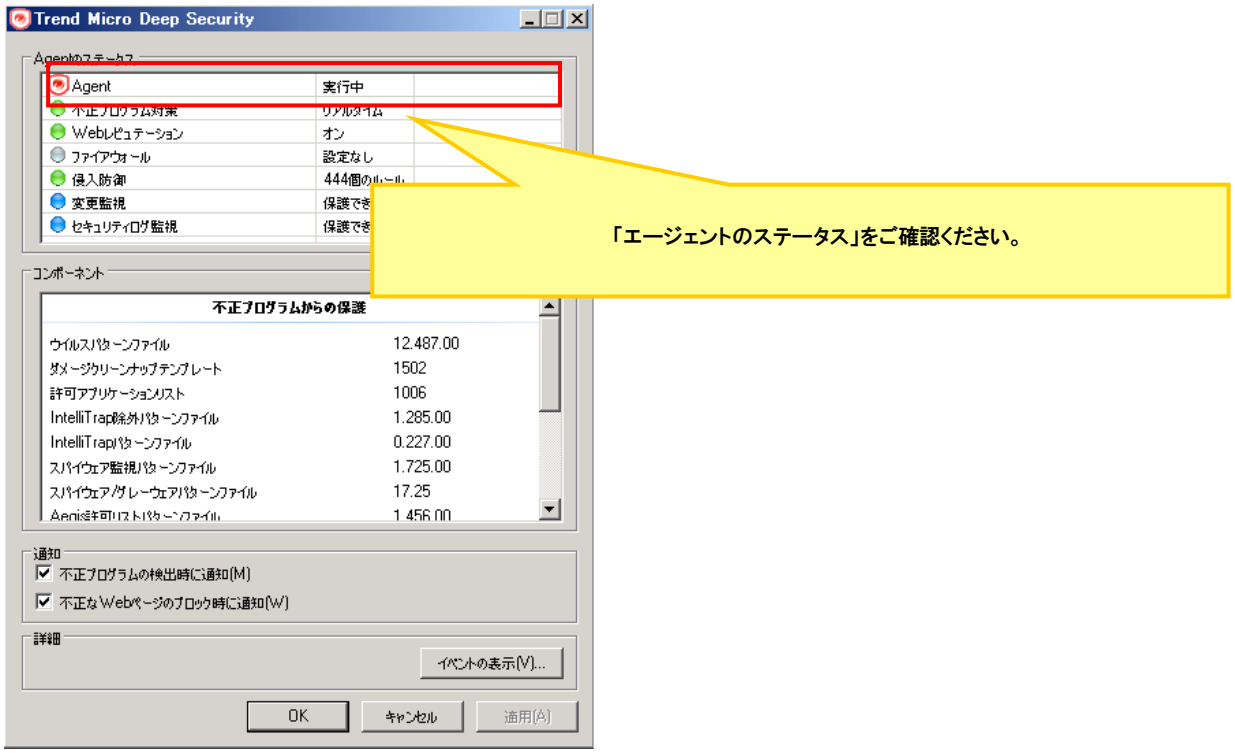
4-1-1.クライアントの状態を確認する

① サーバプロテクションサービスのエージェントのタスクトレイを確認します。

② タスクトレイアイコンからクライアント用のコンソールを開きます。



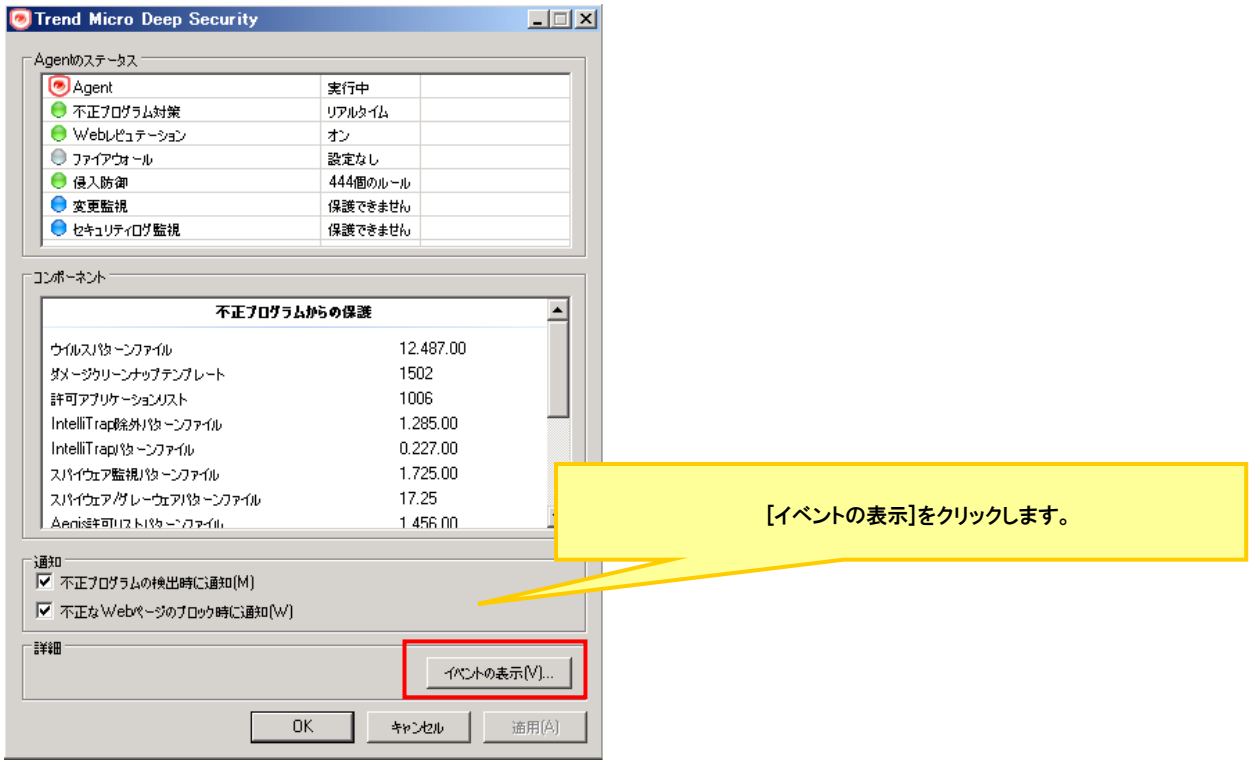
③ クライアント用のコンソールが表示されます。



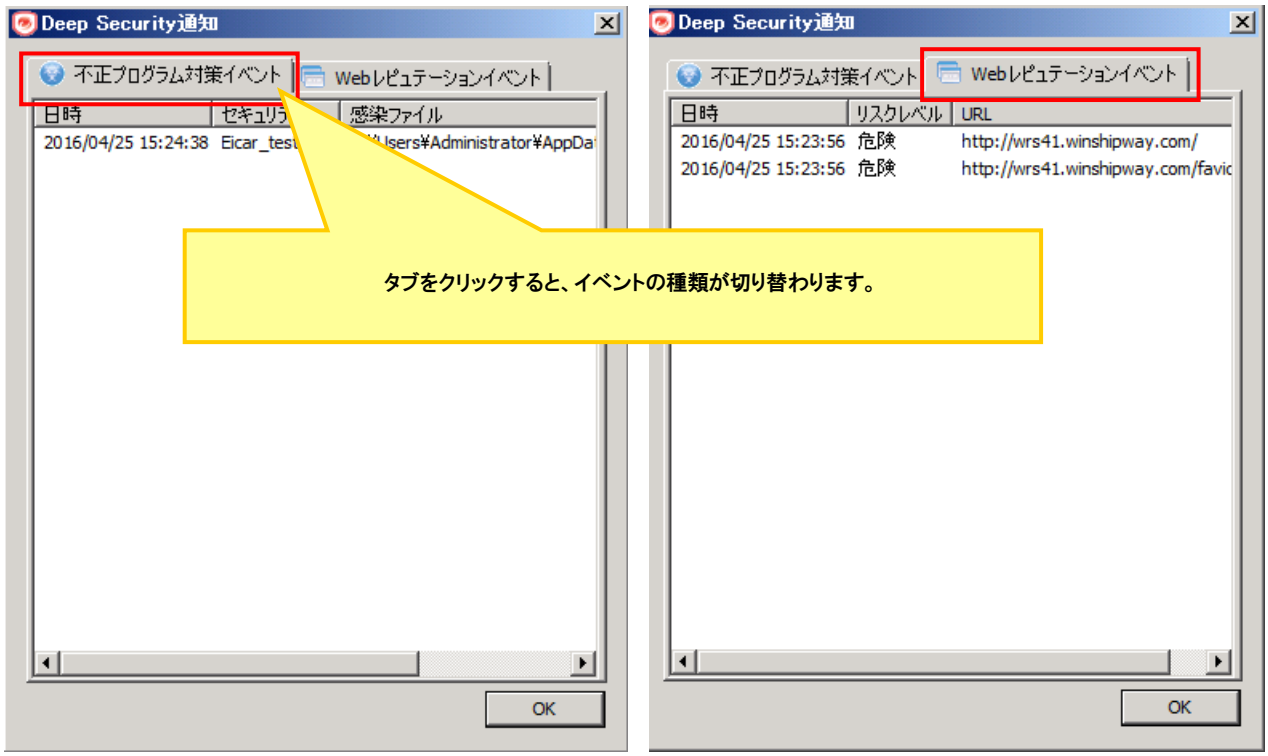
4-1-2.クライアントのイベントを確認する

① 「4-1-1 クライアントの状態を確認する」の手順1～3でクライアント用のコンソールを開きます。

② 通知の画面を開きます。



③ 各イベントのタブをクリックし、イベントの内容を確認します。



MEMO ウイルス感染時の対処方法

「検索結果」に表示される処理が「駆除」、「削除」、「隔離」以外の場合、別途ウイルスの処理を行う必要があります。

参照 5. ウイルス感染時の対処方法

MEMO Webレピュテーションイベントの対処方法

特定の端末でエンドユーザ様に覚えのないWebサイトへのアクセスがブロックされたイベントが発生している場合は、その端末がウイルス感染している可能性があります。調査をご要望の場合は弊社担当エンジニアまでご連絡ください。

5.ウイルス感染時の対処方法

この章では、予約検索やリアルタイム検索などでウイルスが検出された場合の対処を以下に記載します。

5-1.感染の確認

① 管理コンソールもしくはクライアントの[不正プログラム対策イベント]の画面で、「ウイルス名」と「処理」を確認します。

② 処理の欄で、「駆除」、「削除」、「隔離」以外が表示されていないかどうか確認します。
「駆除失敗」などが表示されている場合は、ウイルスに感染している可能性が高いと判断できます。

MEMO 「イベントの参照」方法は3-4-2、4-1-2をご確認下さい。

5-2.トレンドマイクロのホームページによるウイルス情報確認と削除

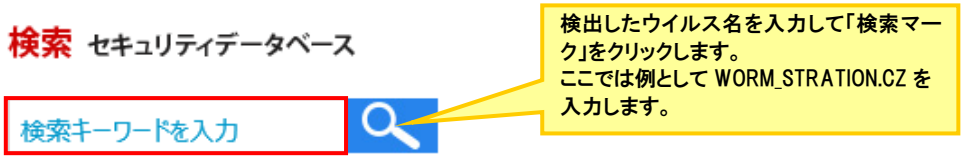
サーバプロテクションサービスではウイルス等の感染を検知すると自動的に駆除を試みます。
前セクションにて感染が確認された場合、以下の手順によりウイルスを駆除します。

ヒント ウイルス情報確認と削除方法

以下の操作は、「WORM_STRATION.EV」というウイルスの対処を例にした作業例です。
なお、トレンドマイクロのホームページ上の操作は2016年5月時点での内容の為、内容が変っている可能性があることをご承知ください。

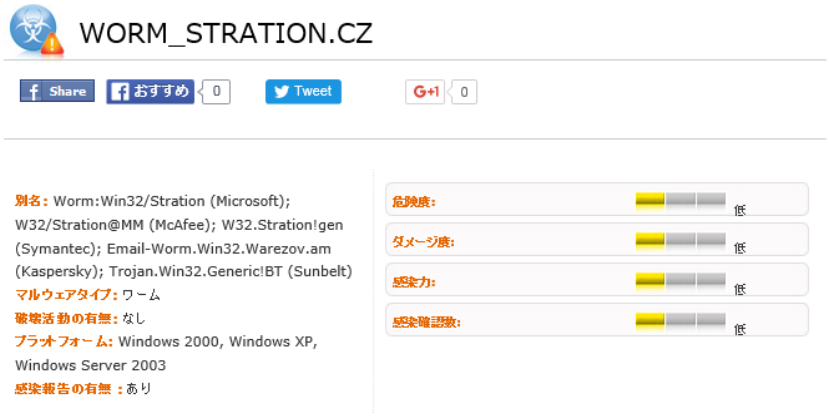
① 別のパソコンから、トレンドマイクロのホームページにアクセスします。
URL は、次の通りです。
http://jp.trendmicro.com/jp/home/
上記 URL より[セキュリティ情報]-[セキュリティデータベース]を開きます。

Ⅰ. ホームページの中の「セキュリティデータベース」でウイルス情報を確認します。
「検索キーワードを入力」と書かれた入力域に、検出したウイルス名を入力し、右の「検索」をクリックします。

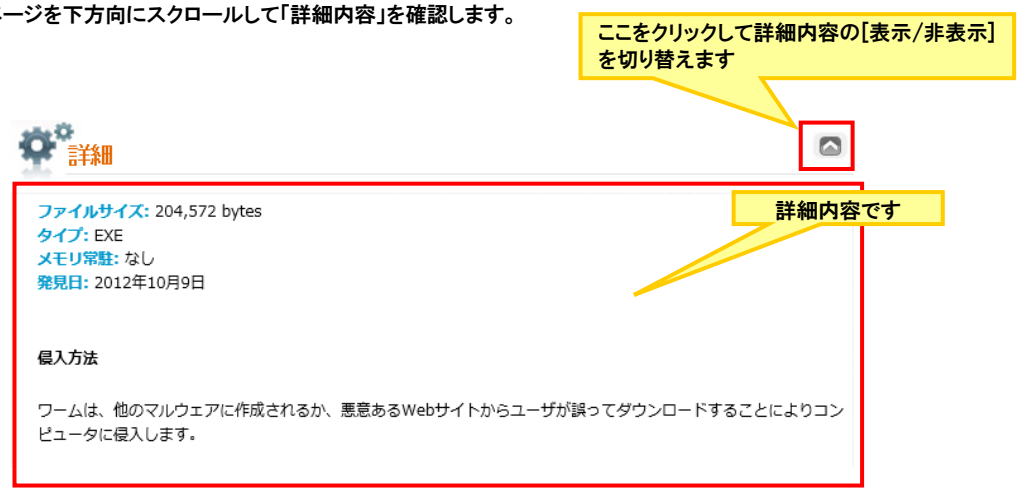


Ⅱ. 検索結果から該当のウイルス情報を選択します。
ウイルスデータベース：検索結果が表示されます。該当のウイルス名をクリックします。

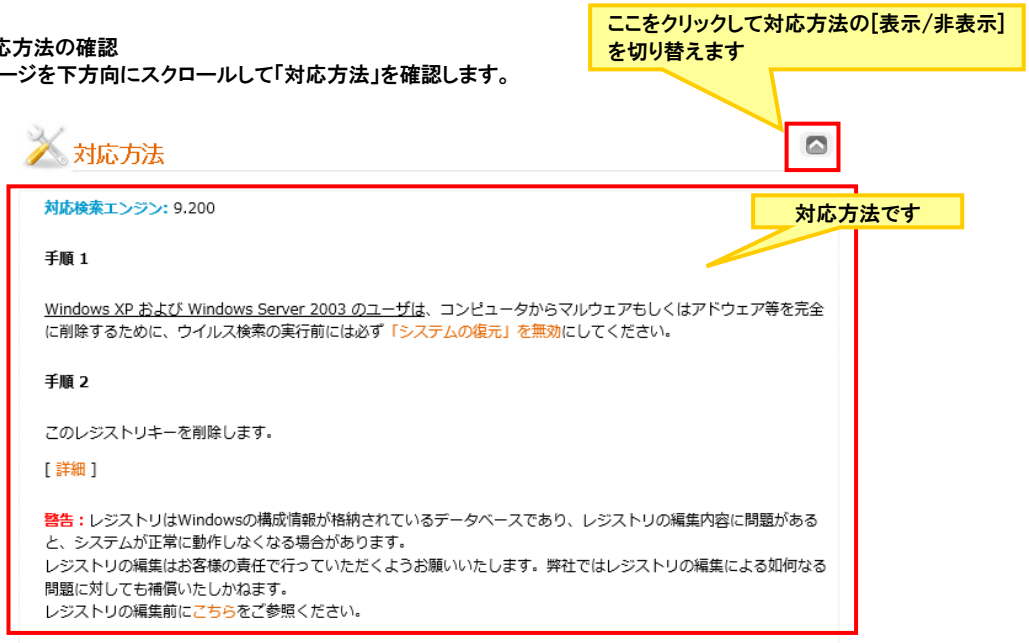
Ⅲ. ウイルス概要の確認
　ウイルスの概要が表示されます。



Ⅳ. 詳細内容の確認
　ページを下方向にスクロールして「詳細内容」を確認します。



Ⅴ. 対応方法の確認
　ページを下方向にスクロールして「対応方法」を確認します。



Ⅵ. ウイルスを削除する。
　「対応方法」のページに記載されている文章をよく読み、その手順に従ってウイルスを削除します。

6.注意

この章では、管理コンソールに関する注意事項を記載します。

6-1.管理コンソールのエラー表示

管理コンソールの特定の項目を選択すると「このページは表示できません」というエラー画面が表示されます。これは、お客様の PC やネットワーク、また、サーバプロテクションサービスのシステム上の問題ではございませんのでご安心ください。

エラー画面を表示する項目

① [ポリシー]-[共通オブジェクト]-[その他]-[不正プログラム対策設定]

② [ポリシー]-[共通オブジェクト]-[リスト]- [ディレクトリリスト]

③ [ポリシー] -[共通オブジェクト]-[リスト]- [ファイルリスト]

④ [ポリシー] -[共通オブジェクト]-[リスト]- [ファイル拡張子リスト]

以下に実際のエラー画面を掲載致します。

7.その他

この章では、お客様の環境変更などについての問い合わせ先を以下に記載します。

7-1.エージェントの追加

お客様が新たにサーバ購入された際や既存のサーバに対して当サービスでのセキュリティ対策をご希望される際は、担当営業かエンジニアまでご連絡ください。

7-2.サーバのリプレース

当サービスでご利用中のサーバをリプレースされる場合や廃棄される際は、担当営業かエンジニアまでご連絡ください。

7-3.設定の変更

当サービスでご利用中のサーバの設定変更をご希望される際は、「サーバプロテクションサービス登録完了のお知らせ」に記載されている連絡先までお問い合わせください。

以下の設定が変更可能となっています。

・推奨スキャン日時

・予約検索の有無

・予約検索日時

・検索除外フォルダの指定

改訂日	改訂内容	版番号
2016年5月7日	初版	1.0
2017年1月24日	お知らせサイトリニューアルに伴う操作手順の変更	1.1
2017年12月1日	管理コンソールのエラー表示に関する記載の修正	1.2

2017年 12月 1日 改訂

SPS-UM-F-20171201